1969

Composition of Binary Quadratic Forms Over Integral Domains.

Bill J. Dulin
Louisiana State University and Agricultural & Mechanical College

COMPOSITION OF BINARY QUADRATIC FORMS OVER INTEGRAL DOMAINS

A Dissertation

Submitted to the Graduate Faculty of the
Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

in

The Department of Mathematics

by
Bill J. Dulin
B.A., Baylor University, May, 1956
M.S., Louisiana State University, August, 1966
May, 1969

ACKNOWLEDGMENT

I wish to thank Professor Hubert S. Butts, under whose direction this dissertation was written, for his assistance, guidance, and encouragement.

TABLE OF CONTENTS

ABSTRACT

This dissertation considers composition of binary quadratic forms over integral domains. The two principal classical definitions of composition of forms with coefficients in Z (the ring of integers) are that of Gauss using bilinear substitutions and that of Dirichlet-Dedekind using "united forms". Our primary object is the investigation of these definitions and the interplay between them.

In Chapter I, the Gaussian concept of composition is extended to Bezout domains with many results being true for more general domains. One of the main results is that a direct compound of two forms is unique up to an equivalence class of forms. It follows that classes of primitive forms are a group under composition when the coefficients of the forms are from a Bezout domain. Throughout this dissertation our primary concern was primitive forms with a fixed nonsquare discriminant over a domain with characteristic not two and often we require the middle coefficients of the forms to be congruent modulo two. However, many of our results are of a more general nature and particularly is this true for Chapter I.

The relationship of "united form" composition to Gaussian composition is investigated in Chapter II. Although "united form" composition implies Gaussian composition, the converse is not known. However, we show several statements are equivalent to "united form" composition holding in a domain where composition holds in the Gaussian sense.

In the third chapter, it is shown that elementary divisor domains have "united form" composition. There are some further necessary and sufficient conditions given for "united form" composition to hold in a Bezout domain. Eight nontrivial examples of elementary divisor domains (EDDs) are given; in fact all the Bezout domains we know are EDDs.

The last chapter is a study of composition in domains that might not be Bezout. We investigate when local information yields global information (i.e., when D_P for P a prime ideal in the domain D yields information about D itself) with respect to composition. One of our main results is that $D[x]$, where D is a PID, is a domain having Gaussian composition. The proof is given in terms of a domain having the property that finitely generated projective modules are free. We also look at domains having the property that each nonzero element is contained in at most a finite number of maximal ideals.

INTRODUCTION

Let D be an integral domain (i.e., a commutative ring without proper divisors of zero) with multiplicative identity, quotient field K, and characteristic not 2. If x_1, y_1 are indeterminants over D, the polynomial $ax_1^2 + bx_1y_1 + cy_1^2 \in D[x_1, y_1]$ is called a <u>binary quadratic form</u> over D and will be denoted $[a,b,c]$. When we use the term form in the paper, we mean a binary quadratic form. We will not distinguish between the form $ax_1^2 + bx_1y_1 + cy_1^2 \in D[x_1, y_1]$ and the form $ax_2^2 + bx_2y_2 + cy_2^2 \in D[x_2, y_2]$ using the same symbol $[a,b,c]$ for both.

If $f = [a,b,c]$, then the <u>matrix</u> of f is the matrix

$$F = \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix}$$

and the discriminant of f is $d = b^2 - 4ac$.

If $f_1 = a_1x_1^2 + b_1x_1y_1 + c_1y_1^2$ is a binary quadratic form over D and

$$(1) \qquad T = \begin{cases} x_1 = a_{11}x_2 + a_{12}y_2 \\ y_1 = a_{21}x_2 + a_{22}y_2 \end{cases}$$

is a linear transformation with coefficients in an overring

R of D (x_2, y_2 indeterminants over R), then T transforms f_1 into a binary quadratic form $f_2 = a_2x_2^2 + b_2x_2y_2 + c_2y_2^2$ over R, where

$$a_2 = a_1a_{11}^2 + b_1a_{11}a_{21} + c_1a_{21}^2$$

$$(1') \qquad b_2 = 2a_1a_{11}a_{12} + b_1(a_{11}a_{22} + a_{12}a_{21}) + 2c_1a_{21}a_{22}$$

$$c_2 = a_1a_{12}^2 + b_1a_{12}a_{22} + c_1a_{22}^2 \quad .$$

If d_i is the discriminant of $f_i (i = 1,2)$ and if the determinant of T is denoted $|T|$ (the same letter T being used to denote the transformation (1) and the matrix (a_{ij}) of the transformation), then $d_2 = |T|^2 \cdot d_1$. If F_i denotes the matrix of f_i $(i = 1,2)$, then the above relationship can be expressed by the equation $T'F_1T = F_2$, where T' denotes the transpose of T, and the discriminant relations follows by the multiplication theorem for determinants.

If the transformation T in (1) has coefficients in D and $|T| = 1$, then the forms f_1 and f_2 are said to be <u>equivalent</u> (in symbols $f_1 \sim f_2$).

The divisor of a binary quadratic form $f = [a,b,c]$ is the ideal (a,b,c) of D generated by the coefficients of f, and f is said to be <u>primitive</u> provided the divisor of f is D.

If d is a <u>nonsquare</u> discriminant of D (i.e.,

$d = b^2 - 4ac$ for $a,b,c \in D$ and d is not the square of an element of D), then $\mathfrak{F}(d)$ will denote the set of all binary quadratic forms over D with discriminant d. The subset of $\mathfrak{F}(d)$ consisting of the primitive forms will be denoted by $\mathcal{P}(d)$. It is clear that the relation $\sim$ defined above is an equivalence relation on $\mathfrak{F}(d)$ and on $\mathcal{P}(d)$; the equivalence class of a form f under $\sim$ will be denoted $\bar{f}$.

The two principal classical definitions of composition of binary quadratic forms with coefficients in Z (the ring of integers) are that of Gauss using bilinear substitutions (see [G, Arts. 235-243] and [S,231-246]), and that of Dirichlet-Dedekind using "united forms" (see [DD], [P,1171-1175]). Investigation of these definitions and the interplay between them over a domain D is the primary object of this paper.

We consider first the Gaussian concept of composition. Although Gauss was concerned with forms having integral coefficients, a careful reading of [G,Arts. 235-243] shows that much of what Gauss did in connection with composition is valid, with certain modifications, for forms with coefficients in a Bezout domain, i.e., a domain in which finitely generated ideals are principal. The problem of composition of binary quadratic forms over a Bezout domain has been recently considered by I. Kaplansky [KA2, 523-530]

using techniques completely different from Gauss; Butts and Estes also have results bearing on this question [BE, 175]. In order to motivate one of the definitions of composition which is used in this dissertation, we present Gauss' approach to composition and, at the same time, give another treatment of composition over a Bezout domain.

A treatment of Bezout domains can be found in [B4] and [GI]. A Bezout domain D with quotient field K is integrally closed in K, i.e., $\alpha \in K$, $\alpha^n + c_1\alpha^{n-1} + \ldots + c_n = 0$ with $c_i \in D$ implies that $\alpha \in D$. For, if $\alpha = \frac{a}{b}$ $(a,b \in D)$, then $(a,b) = (d)$, $a = a_1 d$, $b = b_1 d$, $(a_1,b_1) = D$, $(a_1^n,b_1) = D$, $a_1^n = b_1 (-c_1 a_1^{n-1} - \ldots - c_n)$, and b_1 is a unit in D. It should be noted that Bezout domains are Prüfer domains.

CHAPTER I

TRANSFORMING A FORM INTO A PRODUCT OF FORMS

Gauss based his concept of composition on the notion of transforming a form into a product of two forms by a bilinear transformation. Many of the results that Gauss obtained in this connection are true in an arbitrary domain (characteristic not 2) and most of the rest are true in a Bezout domain. In many cases Gauss' original arguments remain valid; however, in certain cases we give a modified argument in order to obtain the result in the more general setting.

Definition: Let $f_i = a_i x_i^2 + b_i x_i y_i + c_i y_i^2$ be a binary quadratic form with coefficients in a domain D and discriminant d_i for $i = 1,2,3$. We shall say that f_3 is transformable into the product $f_1 f_2$ (an element of $D[x_1,y_1,x_2,y_2]$) provided there exists a bilinear transformation

$$(2) \qquad T = \begin{cases} x_3 = p_0 x_1 x_2 + p_1 x_1 y_2 + p_2 y_1 x_2 + p_3 y_1 y_2 \\ y_3 = q_0 x_1 x_2 + q_1 x_1 y_2 + q_2 y_1 x_2 + q_3 y_1 y_2 \end{cases}$$

with coefficients in D under which $f_3 = f_1 f_2$. Again we will use T to represent (2) and also the matrix

$$\begin{bmatrix} p_o & p_1 & p_2 & p_3 \\ q_o & q_1 & q_2 & q_3 \end{bmatrix} .$$

The six minor determinants of order 2 in T play an important role in this development and we denote them by

$$(3) \qquad D_{ij} = p_i q_j - q_i p_j \qquad (0 \leq i < j \leq 3) .$$

The <u>divisor</u> of T is the ideal of D generated by the D_{ij} and T will be called <u>primitive</u> if the divisor of T is D.

We note that the transformation T in (2) can be considered as a linear transformation

$$(4) \qquad T_1 = \begin{cases} x_3 = (p_o x_1 + p_2 y_1)x_2 + (p_1 x_1 + p_3 y_1)y_2 \\ y_3 = (q_o x_1 + q_2 y_1)x_2 + (q_1 x_1 + q_3 y_1)y_2 \end{cases}$$

with coefficients in $D[x_1, y_1]$, and also as a linear transformation

$$(5) \qquad T_2 = \begin{cases} x_3 = (p_o x_2 + p_1 y_2)x_1 + (p_2 x_2 + p_3 y_2)y_1 \\ y_3 = (q_o x_2 + q_1 y_2)x_1 + (q_2 x_2 + q_3 y_2)y_1 \end{cases}$$

with coefficients in $D[x_2, y_2]$. This approach is used by H. J. S. Smith [S, 229-246].

<u>Remark</u>: We note that if f_3 and f_3' are both transformed into $f_1 f_2$ under the same bilinear transformation T,

then $f_3 \sim f_3'$ since the linear transformation T_1 in (4) has an inverse (it follows from (6) in the proof of Proposition 1 that $|T_1| \neq 0$) in $K(x_1,y_1)$.

Proposition 1: Let $f_i = [a_i,b_i,c_i]$ be a form with discriminant d_i and coefficients in a domain D having quotient field K$(i = 1,2,3)$. If f_3 is transformable into f_1f_2 under T (using the notation of (2) and (3)), then there exist $r_1,r_2 \in K$ such that the following hold:

(a) $d_i = d_3r_i^2$ for $i = 1,2$

(b) $$\begin{cases} D_{01} = a_1r_2,\ D_{03} - D_{12} = b_1r_2,\ D_{23} = c_1r_2 \\ D_{02} = a_2r_1,\ D_{03} + D_{12} = b_2r_1,\ D_{13} = c_2r_1 \end{cases}$$

(c) $$\begin{cases} a_3r_1r_2 = q_1q_2 - q_0q_3, c_3r_1r_2 = p_1p_2 - p_0p_3 \\ b_3r_1r_2 = p_0q_3 + q_0p_3 - p_1q_2 - q_1p_2 \end{cases}$$

Conversely, if f_1 and f_2 are given and there exist $p_i,q_i \in D$ $(i = 1,2,3)$, $r_i \in K$ $(i = 1,2)$ and $a_3,b_3,c_3 \in D$ satisfying (b) and (c), then $[a_3,b_3,c_3]$ is transformable into f_1f_2 under the bilinear transformation determined by the p_i,q_i (as in (2)) and (a) holds.

Proof: Since $f_3 = f_1f_2$ under the linear substitution T_i of (4) and (5) for $i = 1,2$, it follows (see the discussion following (1)) that

(6) $\quad d_3|T_1|^2 = f_1^2 d_2 \quad \text{and} \quad d_3|T_2|^2 = f_2^2 d_1$

where $|T_i|$ is the determinant of the linear transformation T_i. From (4) and (5) it is clear that

(7) $\quad |T_1| = D_{01}x_1^2 + (D_{03} - D_{12})x_1y_1 + D_{23}y_1^2$

(8) $\quad |T_2| = D_{02}x_2^2 + (D_{03} + D_{12})x_2y_2 + D_{13}y_2^2$

Now (a) and (b) follow directly by using (7) and (8) and equating coefficients in (6). To establish (c), consider the inverse transformation T_1^{-1} of T_1 in (4),

$$T_1^{-1} = \frac{1}{r_2 f_1} \begin{bmatrix} q_1x_1 + q_3y_1 & -p_1x_1 - p_3y_1 \\ -q_0x_1 - q_2y_1 & p_0x_1 + p_2y_1 \end{bmatrix}$$

Considering f_1f_2 as a form in x_2, y_2 with coefficients in $D[x_1,y_1]$ and applying the linear transformation T_1^{-1} to f_1f_2, we obtain f_3. Computing the coefficients of the form obtained from f_1f_2 by applying T_1^{-1} (see (1)), and then equating them with a_3,b_3,c_3 we obtain expressions of the following type:

(9) $\quad r_2^2 a_3 f_1 = (a_2q_1^2 - b_2q_0q_1 + c_2q_0^2)x_1 + K_1x_1y_1 + L_1y_1^2$

(10) $\quad r_2^2 b_3 f_1 = K_2x_1^2 + [-2a_2(p_1q_3 + q_1p_3) +$
$b_2(q_1p_2 + q_3p_0 + p_1q_2 + p_3q_0) - 2c_2(q_0p_2 + q_2p_0)]x_1y_1$
$+ L_2y_1^2$

(11) $\quad r_2^2 c_3 f_1 = K_3 x_1^2 + L_3 x_1 y_1 + (a_2 p_3^2 - b_2 p_3 p_2 + c_2 p_2^2) y_1^2$.

Equating the coefficients of x_1^2 in (9), $x_1 y_1$ in (10), and y_1^2 in (11), and performing a rather long calculation, we obtain (c) from (b).

The converse follows directly (by a rather long calculation) by applying the indicated transformation to $[a_3, b_3, c_3]$ and using (b) and (c).

Lemma 2: In a Bezout domain D, $x^2 \equiv y^2 \pmod 4$ implies $x \equiv y \pmod 2$.

Proof: Since $x^2 \equiv y^2 \bmod 4$ implies there exists $k \in D$ such that $x^2 - y^2 - 4k = 0$, it follows that $(x-y)/2$ satisfies $X^2 + yX - k$ where X is an indeterminant over D. Since a Bezout domain is integrally closed, we have $(x-y)/2 \in D$ and hence $x - y = 2\ell$ for some $\ell \in D$.

Lemma 3: If $[a,b,c]$ and $[a',b',c']$ are forms with equal discriminants and coefficients in a Bezout domain D, then $(t) = (a,b,c,a',b',c')$ and $(u) = (a,a',c,c',(b+b')/2,(b-b')/2)$ are equal.

Proof: It is clear that $t \in (u)$. Since the forms $[a/t, b/t, c/t]$ and $[a'/t, b'/t, c'/t]$ have the same discriminant, it follows that $(b/t)^2 \equiv (b'/t)^2 \bmod 4$ and hence $b/t \equiv b'/t \bmod 2$. Consequently $(b \pm b')/2 \equiv 0 \bmod t$ and $u \in (t)$.

Proposition 4: Let $f_i = [a_i, b_i, c_i]$ be a form with discriminant d_i, divisor $(m_i) = (a_i, b_i, c_i)$, and coefficients in a Bezout domain D for $i = 1,2,3$. If f_3 is transformable into $f_1 f_2$ under a bilinear transformation T of divisor (k), then

(a) $(d_1 m_2^2, d_2 m_1^2) = d_3(k)^2$ and

(b) $m_1 m_2 | m_3 k^2$ and $m_3 | m_1 m_2$ (i.e., $(m_3) = (m_1 m_2)$ when $k = 1$).

Proof: Recalling that the content of a polynomial is the ideal generated by its coefficients and that the content of the product of two polynomials is equal to the product of their contents over a Bezout domain, we have from (6) - (8):

(12) $d_3(D_{01}, D_{03} - D_{12}, D_{23})^2 = d_2(m_1)^2$ and

(13) $d_3(D_{02}, D_{03} + D_{12}, D_{13})^2 = d_1(m_2)^2$.

It follows from (a) and (b) of Proposition 1 that the forms $[D_{01}, D_{03} - D_{12}, D_{23}]$ and $[D_{02}, D_{03} + D_{12}, D_{13}]$ have the same discriminant. Applying Lemma 3 and noting that $(x,y)^2 = (x^2, y^2)$ in a Bezout domain, we obtain (a) from (12) and (13) as follows

$$\begin{aligned}(d_1 m_2^2, d_2 m_1^2) &= (d_3(D_{01}, D_{03} - D_{12}, D_{23})^2, \\ &\quad d_3(D_{02}, D_{03} + D_{12}, D_{13})^2) \\ &= d_3(D_{01}, D_{03} - D_{12}, D_{23}, D_{02}, D_{03} + D_{12}, D_{13})^2 \\ &= d_3(k)^2.\end{aligned}$$

The content of f_1f_2 is (m_1m_2), and by applying T to f_3 we obtain a polynomial in $D[x_1,y_1,x_2,y_2]$ such that each coefficient is divisible by m_3. Hence $m_3|m_1m_2$. From (9) we have $a_3r_2^2a_1 = a_2q_1^2 - b_2q_1q_0 + c_2q_0^2$, and since $D_{01} = a_1r_2$, we get $a_3D_{01}^2 = a_1(a_2q_1^2 - b_2q_1q_0 + c_2q_0^2)$ and therefore $m_1m_2|a_3D_{01}^2$. It is easy to show that K_1 and L_1 in (9) are divisible by m_2. It follows from (9) that $m_1m_2|a_3(D_{03} - D_{12})^2$ and $m_1m_2|a_3D_{23}^2$ by equating the coefficients of x_1y_1 and y_1^2 successively. By replacing the transformation T_1^{-1} by T_2^{-1} in the proof of Proposition 1, we obtain equations (9′),(10′), (11′) analogous to (9), (10), (11) in which the roles of f_1 and f_2 have been interchanged, and from (9′) we get $m_1m_2|a_3D_{02}^2$, $m_1m_2|a_3(D_{03} + D_{12})^2$, and $m_1m_2|a_3D_{13}^2$. By the remark after (13) and by Lemma 3, we have

$$(D_{01}^2,(D_{03} - D_{12})^2,D_{23}^2,D_{02}^2,(D_{03} + D_{12})^2,D_{13}^2) =$$

$$(D_{01},D_{03} - D_{12},D_{23},D_{02},D_{03} + D_{12},D_{13})^2 =$$

$$(D_{01},D_{02},D_{03},D_{12},D_{13},D_{23})^2 = (k)^2$$

and $m_1m_2|a_3k^2$. Similarly, using (10), (10′), (11), (11′), we have $m_1m_2|b_3k^2$ and $m_1m_2|c_3k^2$. Hence $m_1m_2|m_3k^2$.

Corollary 5: In Proposition 4, if $d_1 = d_2 = d$, then $d_3 = d$ if and only if $(m_1,m_2) = (k)$.

Lemma 6: Let x,y be elements of a Bezout domain D with

quotient field K and let z be an element of K. If $(x,y) = D$ and $xy = z^2$, then $z \in D$ and there exists a unit $u \in D$ such that ux and $u^{-1}y$ are both squares of elements of D.

Proof: Since D is integrally closed, it follows that $z \in D$. There exists $e \in D$ such that $(x,z) = (e)$. Since $(x,y) = D$ and $xy = z^2$, it follows that $e^2 | x$ in D. Now $(x/e, z/e) = (x/e^2, z/e) = D$ and $(x/e^2)\cdot y = z^2/e^2$ implies $y | (z^2/e^2)$ and $(z^2/e^2) | y$. Hence $u^{-1} = z^2/ye^2$ is a unit of D and $u\cdot x = e^2$ and $u^{-1}y = (z/e)^2$.

Lemma 7: Let d_i, m_i be elements of a Bezout domain D with quotient field K $(i = 1,2)$ and suppose that $d_1 = d_2 s^2$ for $s \in K$. Then there exists $d \in D$ and $r_i \in K$ such that $d_i = dr_i^2$ $(i = 1,2,)$, $(d_1 m_2^2, d_2 m_1^2) = (d)$, $m_1 r_2 \in D$, and $m_2 r_1 \in D$.

Proof: There exists $d' \in D$ such that $(d_1 m_2^2, d_2 m_1^2) = (d')$ and therefore $(d_1 m_2^2/d', d_2 m_1^2/d') = D$. By Lemma 6, there exist $a,b \in D$ and a unit $u \in D$ such that $ud_1 m_2^2/d' = a^2$ and $d_2 m_1^2/ud' = b^2$. Setting $d = ud'$, $r_1 = a/um_2$, and $r_2 = b/m_1$, we have $d_i = dr_i^2$ $(i = 1,2)$ and $(d) = (d')$. Q.E.D.

The proof of the following theorem gives an algorithm (due to Gauss [G,Art. 236]) for finding a form which is transformable into the product of two given forms (provided the ratio of their discriminants is a square) under a

primitive bilinear transformation.

Theorem 8: Let $f_1 = [a_i, b_i, c_i]$ be a form with discriminant d_i, divisor $(m_i) = (a_i, b_i, c_i)$, and coefficients in a Bezout domain D with quotient field K$(i = 1,2)$. In order that there exists a form f with coefficients in D which is transformable into $f_1 f_2$ it is necessary and sufficient that there exists $s \in K$ such that $d_1 = d_2 s^2$.

Proof: The necessity follows from Proposition 1. Conversely, suppose $d_1 = d_2 s^2$ with $s \in K$. By Lemma 7, we have $d \in D$ and $r_1, r_2 \in K$ such that

(14) $d_i = d r_i^2 (i = 1,2)$, $m_1 r_2 \in D$, $m_2 r_1 \in D$

(15) $(d_1 m_2^2, d_2 m_1^2) = (d)$.

It follows from (14) and (15) that

(16) $(m_1 r_2, m_2 r_1) = D$.

We have $a_1 r_2 = m_1 r_2 (a_1/m_1) \in D$, and similarly $b_1 r_2, c_1 r_2, a_2 r_1, b_2 r_1, c_2 r_1$ are elements of D. Let Q_0, Q_1, Q_2, Q_3 be any elements of D such that not all of the following are zero:

$$(17) \begin{cases} Q_1 a_1 r_2 + Q_2 a_2 r_1 + Q_3 (b_1 r_2 + b_2 r_1)/2 = N_0 \\ -Q_0 a_1 r_2 + Q_3 c_2 r_1 - Q_2 (b_1 r_2 - b_2 r_1)/2 = N_1 \\ Q_3 c_1 r_2 - Q_0 a_2 r_1 + Q_1 (b_1 r_2 - b_2 r_1)/2 = N_2 \\ -Q_2 c_1 r_2 - Q_1 c_2 r_1 - Q_0 (b_1 r_2 + b_2 r_1)/2 = N_3 \end{cases}$$

Let $(n) = (N_0, N_1, N_2, N_3)$ and $N_i = nq_i$ for $i = 0,1,2,3$. There exist $P_i (i = 1,2,3,4)$ such that

$$(18) \quad P_0q_0 + P_1q_1 + P_2q_2 + P_3q_3 = 1.$$

Now, define $p_i (i = 1,2,3,4)$ by

$$(19) \quad \begin{cases} P_1a_1r_2 + P_2a_2r_1 + P_3(b_1r_2 + b_2r_1)/2 = p_0 \\ - P_0a_1r_2 + P_3c_2r_1 - P_2(b_1r_2 - b_2r_1)/2 = p_1 \\ P_3c_1r_2 - P_0a_2r_1 + P_1(b_1r_2 - b_2r_1)/2 = p_2 \\ - P_2c_1r_2 - P_1c_2r_1 - P_0(b_1r_2 + b_2r_1)/2 = p_3. \end{cases}$$

Now define a,b,c by

$$(20) \quad \begin{cases} q_1q_2 - q_0q_3 = ar_1r_2, \; p_1p_2 - p_0p_3 = cr_1r_2 \\ p_0q_3 + q_0p_3 - p_1q_2 - q_1p_2 = br_1r_2 \end{cases}$$

We assert that: $a,b,c \in D$, the transformation

$$T = \begin{pmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix}$$

is primitive, and the form $[a,b,c]$ is of discriminant d and is transformable into f_1f_2 under T. The proof of this assertion is the same as that in [G,Art. 236] and will be omitted (the idea being to show that $a,b,c \in D$ and that the converse of Proposition 1 applies.

Remark: We note that the proof of Theorem 8 implies that for each triple d, r_1, r_2 satisfying (14) and (15) there exists a form $[a,b,c]$ of discriminant d which is

transformable into $f_1 f_2$ under a primitive bilinear transformation.

Lemma 9: Let (a_{ij}) be a 2x4 matrix (2 rows, 4 columns) of divisor (k) with entries in a Bezout domain D. Then there exist a primitive 2x4 matrix (a'_{ij}) and a 2x2 matrix H with entries in D such that $(a_{ij}) = H(a'_{ij})$,

$$H = \begin{bmatrix} a & 0 \\ c & b \end{bmatrix}, \quad ab = k.$$

Proof: Let $(a) = (a_{11}, a_{12}, a_{13}, a_{14})$ and $a'_{1j} = a_{1j}/a$ for $j = 1,2,3,4$. There exist $t_j \in D$ $(j = 1,2,3,4)$ such that

$$(21) \qquad \sum_{j=1}^{4} t_j a'_{1j} = 1$$

Define b by $ab = k$ and set $c = \sum_{1}^{4} t_j a_{2j}$.

The six minor determinants of order 2 in (a_{ij}) are $D_{ij} = a_{1i}a_{2j} - a_{2i}a_{1j}$ $(1 \le i < j \le 4)$. Set $D'_{ij} = D_{ij}/a$ for $1 \le i < j \le 4$. Then

$$(22) \qquad (D'_{12}, D'_{13}, D'_{14}, D'_{23}, D'_{24}, D'_{34}) = (b).$$

Set $D''_{ij} = D'_{ij}/b$ for $1 \le i < j \le 4$. Using (21) and (22), an easy calculation shows that $ca'_{1j} - a_{2j} = \sum_{i \neq j} t_i D'_{ji} \equiv 0 \pmod{b}$. Define a'_{2j} by $a'_{2j} = (a_{2j} - ca'_{1j})/b$ for $j = 1,2,3,4$. It

follows that $(a_{ij}) = \begin{bmatrix} a & 0 \\ c & b \end{bmatrix}(a'_{ij})$. The six minor determinants of order 2 in (a'_{ij}) are D''_{ij} for $1 \leq i < j \leq 4$, so that (a'_{ij}) is primitive by (22).

Proposition 10: Let f_i be a binary quadratic form with discriminant d_i and coefficients in a Bezout domain D, and suppose that f_3 is transformable into $f_1 f_2$ under a bilinear transformation T of divisor (k). Then there exists a form f'_3, with coefficients in D and discriminant $d_3 k^2$, and a primitive bilinear transformation T' such that f'_3 is transformable into $f_1 f_2$ under T'.

Proof: If $T = (a_{ij})$, then by Lemma 10 we have $T = HS'$ where $S = (a'_{ij})$ is primitive and

$$H = \begin{bmatrix} a & 0 \\ c & b \end{bmatrix}, \quad ab = k.$$

As in (4), we can interpret T and S as linear transformation T_1 and S_1 respectively

$$T_1 = \begin{pmatrix} a_{11}x_1 + a_{13}y_1 & a_{12}x_1 + a_{14}y_1 \\ a_{21}x_1 + a_{23}y_1 & a_{22}x_1 + a_{24}y_1 \end{pmatrix}, S_1 = \begin{pmatrix} a'_{11}x_1 + a'_{13}y_1 & a'_{12}x_1 + a'_{14}y_1 \\ a'_{21}x_1 + a'_{23}y_1 & a'_{22}x_1 + a'_{24}y_1 \end{pmatrix}$$

and it follows easily that $HS_1 = T_1$ If F_3 denotes the matrix of f_3, then the matrix of the image of f_3 under T_1 is $T'_1 F_3 T_1$ (where T'_1 denotes the transpose of T_1).

Furthermore

$$(23) \qquad T_1'F_3T_1 = (HS_1')'F_3(HS_1) = S_1'(H'F_3H)S_1 \ .$$

Now $H'F_3H$ is the matrix of a binary quadratic form f_3' with coefficients in D and discriminant d_3k^2, and it follows from (23) that f_3' is transformable into f_1f_2 under the primitive bilinear transformation S.

Corollary 11: Let f_i be a binary quadratic form with discriminant d_i and coefficients in a Bezout domain D with quotient field K $(i = 1,2)$. Then there exists a form f_3 with coefficients in D which is transformable into f_1f_2 by a primitive transformation if and only if there exists $s \in K$ such that $d_1 = d_2s^2$.

Proof: Follows from Theorem 8 and Proposition 10.

Remark: We note the following consequence of Theorem 8 and Corollary 11. Let f_i be a given form with discriminant d_i, divisor (m_i), and coefficients in a Bezout domain $(i = 1,2)$. If there exists f_3 transformable into f_1f_2 under a bilinear transformation T of divisor (k), then Proposition 4 implies that $(d_1m_2^2, d_2m_1^2) = d_3(k)^2$, where d_3 is the discriminant of f_3 and the ideal on the left depends only on f_1 and f_2. If there exists one such pair f_3, T, then there exists one with $k = 1$.

Proposition 12: Let f_i be a binary quadratic form with

coefficients in a domain D $(i = 1,2,3)$, and suppose f_3 is transformable into $f_1 f_2$ under T. If f_3' is taken into f_3 and f_i is taken into f_i' $(i = 1,2)$ by linear transformations L_i with coefficients in D $(i = 1,2,3)$, then f_3' is transformable into $f_1' f_2'$ under the transformation

$$L_3 T \begin{bmatrix} r_1 L_2 & u_1 L_2 \\ s_1 L_2 & v_1 L_2 \end{bmatrix}, \text{ where } L_i = \begin{bmatrix} r_i & u_i \\ s_i & v_i \end{bmatrix}$$

$(i = 1,2,3)$.

Proof: If B is an arbitrary bilinear transformation, we denote by B_i the associated linear transformation with coefficients in $D[x_i, y_i]$ $(i = 1,2)$ (see (4) and (5)). Let F_i, F_i' be the matrices of f_i, f_i' respectively $(i = 1,2,3)$, and let M' denote the transpose of a matrix M.

Since $L_3' F_3' L_3 = F_3$, it follows that $(L_3 T_1)' F_3' (L_3 T_1) = T_1' F_3 T_1 = f_1 F_2$. It is easy to check that $L_3 T_1 = (L_3 T)_1$ and consequently f_3' is transformable into $f_1 f_2$ under the bilinear transformation $L_3 T$.

Similarly, $T_1' F_3 T_1 = f_1 F_2$ implies $(T_1 L_2)' F_3 (T_1 L_2) = f_1 L_2' F_2 L_2 = f_1 F_2'$; since $T_1 L_2 = S_1$, where

$$S = T \begin{bmatrix} L_2 & N \\ N & L_2 \end{bmatrix}, \quad N = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

it follows that f_3 is transformable into $f_1 f_2'$ under S.

It follows in the same manner that f_3 is transformable into $f_1' f_2$ under the bilinear transformation

$$R = T\begin{bmatrix} r_1 I & u_1 I \\ s_1 I & v_1 I \end{bmatrix} \quad , \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad ;$$

combining these three cases, the proof is complete.

Q.E.D.

It should be noted that

if $$L_3\, T\begin{bmatrix} r_1 L_2 & u_1 L_2 \\ s_1 L_2 & v_1 L_2 \end{bmatrix} =$$

$$\begin{bmatrix} p_0' & p_1' & p_2' & p_3' \\ q_0' & q_1' & q_2' & q_3' \end{bmatrix}$$

and if $D_{ij}' = p_i' q_j' - q_i' p_j' \qquad (0 \le i < j \le 3)$

then

$$(a') \quad d_i' = d_3'\, r_i^2\, (|L_i|/|L_3|)^2 \quad (i = 1,2)$$

$$(b') \begin{cases} D_{01}' = a_1' r_2 |L_2| \,, D_{03}' - D_{12}' = b_1' r_2 |L_2| \,, D_{23}' = c_1 r_2 |L_2| \\ D_{02}' = a_2' r_1 |L_1| \,, D_{03}' + D_{12}' = b_2' r_1 |L_1| \,, D_{13}' = c_2 r_1 |L_1| \end{cases}$$

$$(c') \begin{cases} a_3'(r_1|L_1|)(r_2|L_2|) = q_1' q_2' - q_0' q_3' \,, c_3'(r_1|L_1|)(r_2|L_2|) \\ = p_1' p_2' - p_0' p_3' \,, b_3'(r_1|L_1|)(r_2|L_2|) = p_0' q_3' + q_0' p_3' - p_1' q_2' - q_1' p_2' \end{cases}$$

where r_i $(i = 1,2)$ are as in Proposition I.1.

Remark: If f_3 is transformable into $f_1 f_2$, then it is clear that f_3 is not unique. In fact, the best that can be hoped would be uniqueness within the equivalence relation $\sim$. Can we determine satisfactory restrictions which allow us to obtain a unique "product" class $\bar{f}_3$ under $\sim$, given $\bar{f}_1$ and $\bar{f}_2$? The remark following Corollary 11 suggests the following definition of Gauss [G, Art. 235] as a first step in this direction.

Definition: The form f_3 is a compound (or, a composite) of the forms f_1 and f_2 provided f_3 is transformable into $f_1 f_2$ by a primitive bilinear transformation.

Remark: Let $f = [a,b,c]$ be a compound of f_1 and f_2 by a transformation T, and let T* be the transformation obtained by replacing the second row q_0, q_1, q_2, q_3 of T by $-q_0, -q_1, -q_2, -q_3$. Then $f^* = [a,-b,c]$ is a compound of f_1 and f_2 by the primitive transformation T* and in general f_3 is not equivalent to f_3^*. Gauss dealt with this difficulty (over the ring of integers) by introducing the notion of a direct compound, i.e. a compound such that the primitive transformation had the property that r_1, r_2 in Proposition 1 were positive (see [G, Art. 235] and [BE, 155]. In view of Proposition 1, it is clear that a choice of signs of r_1, r_2 is essential for uniqueness. Obviously this

situation presents a more serious difficulty over a Bezout domain, but a rather general treatment could be given by using the technique of [BE, 163-164]. However, there is a case in which this difficulty can be dealt with for Bezout domains in the same manner as the integers - namely, the case in which the discriminants of all forms considered are equal. In this case $r_i^2 = 1$ for $i = 1,2$ and we can make a choice of signs. We choose the latter approach and make the following definition.

Definition: Let $f_i \in \mathfrak{F}(d)$ for $i = 1,2,3$. We say that f_3 is a direct compound of f_1 and f_2 provided f_3 is a compound of f_1 and f_2 under a (primitive) transformation T such that r_1 and r_2 in Proposition 1 are both equal to 1 (i.e. $|T_i| = f_i$ for $i = 1,2$ - see (4), (5) and Proposition 1).

Remark: We emphasize that our definition of direct compound requires that the three forms involved have the same discriminant, while the corresponding definition of Gauss did not require this restriction [G, Art. 235]; however Gauss ultimately reduced his considerations to the equal discriminant case [G, Arts. 242-244].

Theorem 13: Let $f_i = [a_i,b_i,c_i]$ be a form of discriminant d with divisor $(m_i) = (a_i,b_i,c_i)$ and coefficients in a Bezout domain D $(i = 1,2)$. In order that there exist a

direct compound f_3 of f_1 and f_2, it is necessary and sufficient that $(m_1,m_2) = D$. (The corresponding condition over the integers for forms of different discriminants is that the ratio of the discriminants of f_1 and f_2 be a rational square [G, Art. 236]).

Proof: If there is a direct compound f_3 of f_1 and f_2, then $(m_1,m_2) = D$ by Corollary 5.

The sufficiency follows by Theorem 8.

Q.E.D.

Lemma 14: Let (a_{ij}) and (b_{ij}) be two 2xn matrices $(n \geq 2)$ with entries from a domain D. Set $D_{ij} = a_{1i}a_{2j} - a_{2i}a_{1j}$ and $D'_{ij} = b_{1i}b_{2j} - b_{2i}b_{1j}$ $(1 \leq i < j \leq n)$. Suppose $(D_{12}D_{13}, \ldots, D_{n-1\,n}) = D$ and $D'_{ij} = k D_{ij}$ $(1 \leq i < j \leq n)$. Then there exists a 2x2 matrix H with entries in D such that $H(a_{ij}) = (b_{ij})$ and $|H| = k$.

Proof: See [G, Art. 234].

Theorem 15: If f_3 and f'_3 are both direct compounds of f_1 and f_2, then $f_3 \sim f'_3$, i.e. a direct compound is unique up to an equivalence class.

Proof: If f_3 is transformed into f_1f_2 by T and f'_3 is transformed into f_1f_2 by T', then T and T' satisfy the hypothesis of Lemma 14 (with $n = 4$, $k = 1$) by taking $r_1 = r_2 = 1$ in (b) of Proposition 1. Hence there exists

a 2x2 matrix H with entries in D such that $HT = T'$ and $|H| = 1$. If F_3' denotes the matrix of f_3', it follows as in the proof of Proposition 10 that the form with matrix $H'F_3'H$ (H' the transpose of H) is taken into f_1f_2 under T, and therefore must be f_3 (see the remark preceeding Proposition 1). Since $|H| = 1$, it follows that $f_3 \sim f_3'$.

Definition: If f is a compound of f_1 and f_2 and f' is a compound of f and f_3, then we say f' is a compound of $(f_1f_2)f_3$. A direct compound of $(f_1f_2)f_3$ is defined by adding the word direct before compound everywhere in the preceeding sentence.

Proposition 16: If f is a direct compound of $(f_1f_2)f_3$ and f' is a direct compound of $(f_1f_3)f_2$, then $f \sim f'$.

Proof: For a proof see [G, Art. 240].

Corollary 17: If f is a direct compound of $(f_1f_2)f_3$ and f' is a direct compound of $f_1(f_2f_3)$ and if there exists a direct compound of $(f_1f_3)f_2$, then $f \sim f'$..

Proof: Immediate from Proposition 16 since

$$f_2f_3 = f_3f_2 \quad \text{and} \quad (f_2f_3)f_1 = f_1(f_2f_3).$$

Lemma 18: Let $f_i = [a_i,b_i,c_i]$ be a form with coefficients in a domain D ($i = 1,2,3$). If f_3 is a direct compound of f_1f_2, then $b_1 \equiv b_2 \equiv b_3 \bmod (2)$.

Proof: Immediate using (b) and (c) of Proposition 1 and noting that $r_1 = r_2 = 1$.

Proposition 19: If $f = [a,b,c] \in \mathfrak{F}(d)$, then $I = [1,b,ac] \in \mathfrak{F}(d)$ is a form such that f is a direct compound of $I \cdot f$. Furthermore, any form $f_1 = [a_1,b_1,c_1] \in \mathfrak{F}(d)$ that represents 1 (i.e., $1 = a_1s^2 + b_1st + c_1t^2$ for $s,t \in D$) is equivalent to $[1,b,ac]$ provided $b \equiv b_1 \pmod 2$.

Proof: The desired transformation is

$$\begin{bmatrix} 1 & 0 & 0 & -c \\ 0 & 1 & a & b \end{bmatrix} .$$

Since $1 = a_1s^2 + b_1st + c_1t^2$, it follows that $(s,v) = D$, $su + vt = 1$ for $u,v \in D$, and $[a_1,b_1,c_1]$ is equivalent to a form of the type $[1,b',c']$ (under the linear transformation $\begin{bmatrix} s & -v \\ t & u \end{bmatrix}$), where $b_1 = b' + 2k$ for $k \in D$ (see (1')). Since $b \equiv b_1 \pmod 2$, we have $b = b' + 2k'$ for $k' \in D$. Applying the transformation $\begin{bmatrix} 1 & k' \\ 0 & 1 \end{bmatrix}$ to $[1,b',c']$, and using the fact that all forms considered belong to $\mathfrak{F}(d)$, we obtain $[1,b,ac]$.

Proposition 20: If $[a,b,c] \in \mathfrak{G}(d)$, then $[c,b,a] \in \mathfrak{G}(d)$ and $[ac,b,1]$ is a direct compound of $[a,b,c][c,b,a]$.

The desired transformation is $\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & a & c & b \end{bmatrix}$.

Proposition 21: Suppose $f_i, f_i' \in \mathfrak{F}(d)$ $(i = 1,2,3)$, f_3 is a direct compound of $f_1 f_2, f_3'$ is a direct compound of $f_1' f_2'$, and that $f_i \sim f_i'$ $(i = 1,2)$. Then $f_3 \sim f_3'$, and if $f \sim f_3$, then f is a direct compount of $f_1 f$.

Furthermore, if f_3 is transformed into $f_1 f_2$ by the bilinear transformation T, and if f_3' is transformed into $f_1' f_2'$ by the bilinear transformation S, if f_i is transformed into f_i' by the linear transformation $L_i (i = 1,2,3)$, and if f is transformed into f_3 by the linear transformation K, then

$$S = L_3^{-1} T \begin{bmatrix} r_1 L_2 & u_1 L_2 \\ s_1 L_2 & v_1 L_2 \end{bmatrix} \text{ where } L_1 = \begin{bmatrix} r_1 & u_1 \\ s_1 & v_1 \end{bmatrix} ,$$

L_3^{-1} is the inverse of L_3 and f is transformed into $f_1 f_2$ by the bilinear transformation KT.

Proof: By Proposition 12 and the comment directly after it, setting $r_i = |L_i| = 1$ $(i = 1,2,3)$ and $L_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, it follows that f_3 is a direct compound of $f_1' f_2'$ and hence $f_3 \sim f_3'$ by Theorem 15. If $f \sim f_3$ and if f_3 is a direct compound of $f_1 f_2$, then from Proposition 12

setting $r_i = |L_i| = 1 \quad (i = 1,2,3)$, $L_i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (i = 1,2)$,

and temporarily setting $K = L_3$, it follows that f is a direct compound of $f_1 f_2$. The other statements follow immediately.

Definition: Let $f_i \in \mathfrak{F}(d)$ for $i = 1,2,3$. If f_3 is a direct compound of $f_1 f_2$, then we define the compound of the classes $\bar{f}_1, \bar{f}_2$ to be $\bar{f}_3 = \bar{f}_1 \bar{f}_2$ (and we say that $\bar{f}_3$ is found by composition from $\bar{f}_1$ and $\bar{f}_2$)

We denote by $G_d(D) = G_d$ the collection of equivalence classes determined by $\sim$ on $\mathcal{P}(d)$.

Definition: We say that D is a G domain provided that any two primitive forms with equal discriminants and coefficients in D have a direct compound. Unless otherwise stated we will assume the discriminant to be nonsquare.

Theorem 22: If D is a G-domain, then G_d is an Abelian group under composition.

Proof: Since D is a G-domain, it follows by Proposition 21 that composition is a well defined operation on elements of G_d. By Corollary 17, the associative law holds; by Proposition 19, G_d has an identity; by Proposition 20, each element of G_d has an inverse; and it is trivial that the elements of G_d commute.

Theorem 24: If D is a Bezout domain, then D is a G-domain.

Proof: This is an immediate consequence of Theorem 8.

Remark: An example is given in [BE, 177] of a Noetherian, 2-dimensional, unique factorization domain D which is not a G-domain; in fact, there is a primitive form f with coefficients in D such that no direct compound exists for ff.

CHAPTER II

COMPOSITION OF BINARY QUADRATIC FORMS

Composition of binary quadratic forms in the tradition of Dirichlet and Dedekind is called composition by "united forms". Two forms are called united if they have coprime divisors and the following configuration:

$$f = [a,b,a'c],\ g = [a',b,ac] \quad a,a',b,c \in D.$$

It is easily checked that $h = [aa',b,c]$ is a direct compound of the united forms $f = [a,b,a'c]$ and $g = [a',b,ac]$ under the primitive bilinear transformation

$$T = \begin{bmatrix} 1 & 0 & 0 & -c \\ 0 & a & a' & b \end{bmatrix}$$

As in the case of Gaussian composition, the class $\bar{h}$ is called the compound of the classes $\bar{f}$ and $\bar{g}$ (or, $\bar{h}$ is said to be obtained from $\bar{f},\bar{g}$ by composition). If $\bar{h}'$ is the compound of the united forms f',g' where $f' \in \bar{f}$ and $g' \in \bar{g}$, then it is clear that $\bar{h} = \bar{h}'$ since the direct compound is unique to within an equivalence class of $\sim$. Hence the compound $\bar{h}$ is independent of the united forms chosen as representatives from $\bar{f}$ and $\bar{g}$; furthermore the compound $\bar{h}$ obtained by united forms is the same as that obtained by the Gauss method.

Definition: A domain is called a $\mathcal{B}$-domain (or, is said to have property $\mathcal{B}$) provided the following holds: if C_1 and C_2 are any two classes of primitive forms of the same discriminant, then there exist united forms f,g such that $f \in C_1, g \in C_2$.

Theorem 1: If D is a domain in which every nonzero element is contained in a finite number of maximal ideals and such that $x^2 \equiv y^2 (\mathrm{mod}\ 4)$ implies $x \equiv y (\mathrm{mod}\ 2)$ in D, then D is a $\mathcal{B}$-domain.

Proof: See [BE, 162].

Corollary 2: A Dedekind domain is a $\mathcal{B}$-domain. (In particular, the ring of integers is a $\mathcal{B}$-domain).

Proposition 3: If D is a $\mathcal{B}$-domain, then D is a G-domain.

Proof: If $f,g \in P(d)$, then there exist united forms f',g' such that $f' \in \bar{f}$, $g' \in \bar{g}$. There exists a direct compound h' of $f'g'$ (see the comment following the definition of united forms), and it follows by Proposition I.21 that h' is a direct compound of fg.

Remark: We do not know if the converse to the above theorem is true or not.

Remark: The origin of the concept of united forms is usually attributed to either Dedekind or Dirichlet ([BE, 156],

[BP, 24], [KA 2], [D2, 66], [P]). In treating composition in [D 1] Dickson used the "united form" approach, and this seems to have been the accepted procedure since the time of Dedekind for quadratic forms over the integers. The reason for the rather general acceptance of the united form method of composition seems to be the following: For forms with integral coefficients, a fairly easy method can be derived for producing united forms in given classes (see [D 1] and [P]), and with united forms the direct compound is obtained immediately. Two comments seem to be in order: First, a rather careful reading of [G, Arts. 168, 228, 242-244] indicates that Gauss must have been essentially aware of the technique of united forms and used it in working with examples; and second, the Gauss algorithm (see Theorem 8) as used by Gauss in [G, Arts. 242-244] seems to be as easy to use as the method of computing united forms.

Lemma 4: Let D be a domain such that the ideal $(m,t_1,t_2,\ldots,t_n) = D$ and such that $t_r q_s - q_r t_s \in (m)$ $(r,s = 1,2,\ldots,m)$. Then there exists a unique element B of D modulo (m) such that

$$t_1 B \equiv q_1,\ t_2 B \equiv q_2,\ldots,t_n B \equiv q_n \bmod(m).$$

Proof: Follows by [D1, 134].

Lemma 5: Let D be a domain with $b \equiv b' \bmod (2)$, $b^2 \equiv d \bmod (4a)$, $b'^2 \equiv d \bmod (4a')$, and $(a,a',(b+b')/2) = D$. Then there exists a unique $B \bmod (2aa')$ such that $B \equiv b \bmod (2a)$, $B \equiv b' \bmod (2a')$, $B^2 \equiv d \bmod (4aa')$. Furthermore, $(a,a',B) = D$.

Proof: Follows by [D1, 134-135].

Definition: A domain D has property C provided $a^2 \equiv b^2 \bmod (4)$ implies $a \equiv b \bmod (2)$ for a,b arbitrary elements of D.

Definition: A matrix U is called unimodular provided $|U| = 1$.

Lemma 6: Let $U = (u_{ij})$, V, $W = (w_{ij})$ be 2x2 matrices, and let $T = (t_{ij})$ be a 2x4 matrix with entries in a domain D. Let

$$U\left(w_{11}\begin{bmatrix} t_{11} & t_{12} \\ t_{13} & t_{14} \end{bmatrix} + w_{12}\begin{bmatrix} t_{21} & t_{22} \\ t_{23} & t_{24} \end{bmatrix}\right) = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$$

and

$$V\left(w_{21}\begin{bmatrix} t_{11} & t_{12} \\ t_{13} & t_{14} \end{bmatrix} + w_{22}\begin{bmatrix} t_{21} & t_{22} \\ t_{23} & t_{24} \end{bmatrix}\right) = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} .$$

Then

$$WT\begin{bmatrix} u_{11}V & u_{21}V \\ u_{12}V & u_{22}V \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \end{bmatrix} .$$

Proof: Follows by a direct calculation.

Theorem 7: If D is a domain with property G, then the following are equivalent.

1. The domain D has property $\mathcal{B}$.
2. If $f_i \in \mathcal{P}(d)$ $(i = 1,2)$, then there exists $f_i' = [a_i', b_i', c_i'] \in \mathcal{P}(d)$ such that $f_i' \sim f_i$ $(i = 1,2)$ and $(a_1', a_2', (b_1'+b_2')/2) = D$.
3. If $f_i \in \mathcal{P}(d)$ $(i = 1,2)$, then there exist f_i' $(i = 1,2,3)$ and T with entries from D such that $f_i' \sim f_i$ $(i = 1,2)$ and f_3' is a direct compound of $f_1'f_2'$ under

$$T = \begin{bmatrix} 1 & 0 & 0 & p_3 \\ 0 & q_1 & q_2 & q_3 \end{bmatrix} .$$

4. If $f_i = [a_i, b_i, c_i] \in \mathcal{P}(d)$ $(i = 1,2,3)$ and f_3 is a direct compound of f_1f_2 under T, then there exist U, V, and W, 2×2 matrices in D, such that

$$WT \begin{bmatrix} rV & uV \\ sV & vV \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & p_3 \\ 0 & q_1 & q_2 & q_3 \end{bmatrix}$$

where the last matrix has entries from D and $U = \begin{bmatrix} r & u \\ s & v \end{bmatrix}$.

5. If $f_i = [a_i,b_i,c_i] \in \mathcal{P}(d)$ $(i = 1,2,3)$ and if f_3 is a direct compount of f_1 and f_2 by

$$T = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix},$$

then there exist $\alpha,\beta \in D$ and $U,V,2\times2$ unimodular matrices with entries in D such that $(\alpha,\beta) = D$ and

$$V\left(\alpha \begin{bmatrix} p_0 & p_1 \\ p_2 & p_3 \end{bmatrix} + \beta \begin{bmatrix} q_0 & q_1 \\ q_2 & q_3 \end{bmatrix}\right) \cdot U$$

$$= \begin{bmatrix} h & 0 \\ 0 & k \end{bmatrix}$$

where $h,k \in D$, $h|k$, $k \neq 0$.

Proof: 1)$\Rightarrow$ 2) Since D has property $\mathcal{D}$, we can assume $f_1' = [a_1,b,a_2c]$ and $f_2' = [a_2,b,a_1c]$. Since f_1 and f_2 are primitive it follows that $(a_1,a_2,b) = D$.

2)$\Rightarrow$ 3) Suppose $f_i = [a_i,b_i,c_i] \in \mathcal{P}(d)$ $(i = 1,2)$ and $(a_1,a_2,(b_1 + b_2)/2) = D$. Then the conditions of Lemma 2 are satisfied and hence there exists a unique $B \bmod (2a_1a_2)$ such that $B^2 - d = 4a_1a_2C$ (for $C \in D$), $B = b_1 + 2a_1k$ (for $k \in D$), and $B = b_2 + 2a_2\ell$ (for $\ell \in D$). Therefore, $[a_1,b_1,c_1] \sim [a_1,b_1 + 2a_1k, a_1k^2 + b_1k + c_1]$ $= [a_1,B,a_2C]$ and $[a_2,b_2,c_2] \sim [a_2,B,a_1C]$. It follows that $[a_1a_2,B,C]$ is a direct compound of $[a_1,B,a_2C]$ and

$[a_2, B, a_1 C]$ under

$$T = \begin{bmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{bmatrix} .$$

3)⇒4) Immediate from Proposition I.21.

4)⇒5) Suppose that $U = \begin{bmatrix} r & u \\ s & v \end{bmatrix}$, $V = \begin{bmatrix} m & k \\ n & \ell \end{bmatrix}$,

and $W = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ are unimodular matrices with entries from D and that

$$(6) \quad WT \begin{bmatrix} rV & uV \\ sV & vV \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & P_3^* \\ 0 & q_1^* & q_2^* & q_3^* \end{bmatrix} .$$

It follows from (6) and Lemma 6 that

$$U' \left(\alpha \begin{bmatrix} p_0 & p_1 \\ p_2 & p_3 \end{bmatrix} + \beta \begin{bmatrix} q_0 & q_1 \\ q_2 & q_3 \end{bmatrix} \right) V = \begin{bmatrix} 1 & 0 \\ 0 & p_3^* \end{bmatrix} .$$

Now $f_i \sim f_i^*$ $(i = 1,2,3)$ under U,V,W respectively and f_3' is a direct compound of $f_1^* f_2^*$ under the transformation in (6) (see Proposition I.12 and Proposition I.21). It might be noted that $f_1^* = [q_1^*, q_3^*, -q_2^* p_3^*]$. Since the discriminant d is not a square $p_3^* \neq 0$. Since W is unimodular, $(\alpha, \beta) = D$.

5)⇒1) If $f_i \in \mathcal{O}(d)$ $(i = 1,2)$, then there exists $f_3 \in \mathcal{O}(d)$ such that f_3 is a direct compound of $f_1 f_2$

under a bilinear transformation

$$T = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix} .$$

Since $(\alpha,\beta) = D$, we have $\gamma,\delta \in D$ such that $\alpha\delta - \beta\gamma = 1$. Then 5) and Lemma 6 imply that

$$(7) \qquad S = WT \begin{bmatrix} rV & uV \\ sV & vV \end{bmatrix} = \begin{bmatrix} h & 0 & 0 & k \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix} ,$$

where $V' = \begin{bmatrix} r & u \\ s & v \end{bmatrix}$ and $W = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$.

Since S is a primitive transformation and $h|k$, we have $D = (hq_1, hq_2, hq_3 - q_0k) \subset (h)$, and h is a unit in D. Let

$$(8) \qquad T^* = \begin{bmatrix} 1 & 0 \\ -hq_0 & 1 \end{bmatrix} \begin{bmatrix} h^{-1} & 0 \\ 0 & h \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 & 0 & h^{-1} & k \\ 0 & hq_i & hq_0 & hq_3 - q_0 & k \end{bmatrix}$$

As in the proof of 4)$\Rightarrow$5), $f_i \sim f_i^*$ $(i = 1,2,3)$ and f_3^* is a direct compound of $f_1^* f_2^*$ under T^* ; furthermore, $f_1^* = [hq_1, hq_3 - q_0k, -h^{-1}khq_2]$ and $f_2^* = [hq_2, hq_3 - q_0k, -h^{-1}khq_1]$ are united.

Theorem 8: If $\{D_\alpha\}_{\alpha\in A}$ (A an index set) and D are domains such that the D_α form a net and each D_α is a G-domain ($\mathfrak{H}$-domain) and if $D = \bigcup_{\alpha\in A} D_\alpha$, then D is a G-domain ($\mathfrak{H}$-domain).

(By a net, we mean any two elements of $\{D_\alpha\}_{\alpha\in D}$

are contained in a third).

Proof: If $f_i = [a_i, b_i, c_i] \in \varphi(d)$ $(i = 1,2)$ with coefficients in D, then since $D = \cup D_\alpha$ and since $F = \{a_1, a_2, b_1, b_2, c_1, c_2\}$ is a finite set it follows that there exists $\beta \in A$ such that $F \subset D_\alpha$. Hence f_1 and f_2 are elements of $\varphi(d)$ with coefficients in D_β.

If D_β is a G-domain ($\beta \in A$), then there exists $f_3 = [a_3, b_3, c_3]$ with coefficients in D_β such that f_3 is a direct compound of f_1 and f_2. It follows that f_3 is a direct compound of f_1 and f_2 in D since $D_\beta \subset D$. Thus D is a G-domain.

If D_α is a $\mathcal{B}$-domain ($\alpha \in A$), then $f_1 \sim [a_1', b, a_2'c]$ and $f_2 \sim [a_2', b, a_1'c]$ with coefficients in D_β and hence in D. Thus D is a $\mathcal{B}$-domain.

CHAPTER III

FURTHER RESULTS IN BEZOUT DOMAINS

In this chapter, we will examine when a Bezout domain is a $\mathcal{D}$-domain. As of now, we are unable to show whether or not every Bezout domain is a $\mathcal{D}$-domain. Every example of a bezout domain that we know of is not only a $\mathcal{D}$-domain, they are in fact elementary divisor rings (which we now define).

Definition: A ring R with the property that every matrix can, by multiplication with matrices of unit determinant, be reduced to a diagonal matrix such that each element of the main diagonal divides the one to its lower right is called an elementary divisor ring.

In [KA1, 471-472], it is shown that in a commutative ring if all 1x2, 2x1, and 2x2 matrices can be diagonalized as in the above definition, then the ring is an elementary divisor ring. It is easy to see that all 1x2 and 2x1 matrices over a Bezout domain can be diagonalized by multiplying by unimodular matrices. It follows easily for 2x2 matrices that the diagonalization can be realized by multiplying by unimodular matrices. Furthermore, [KA1, 472] shows that if all the divisors of zero of a ring R are in the Jacobson

radical (i.e., the intersection of all maximal ideals), then R is an elementary divisor ring if and only if (1) each finitely generated ideal is principal and (2) if $(a,b,c) = R$, then there exist $p,q \in R$ such that $(pa, pb + qc) = R$. Since we are interested in domains, we will define an elementary divisor domain to be an elementary divisor ring that is a domain.

Theorem 1: If D is an elementary divisor domain, then D is a $\mathscr{B}$-domain.

Proof: Since D is Bezout, if f_1 and f_2 are two forms in $\mathscr{O}(d)$, then there exists f_3 a direct compound of f_1 and f_2 under a transformation

$$T = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix} .$$

Since the discriminant d is nonsquare it follows that

$$P = |M| = \left| \begin{bmatrix} p_0 & p_1 \\ p_2 & p_3 \end{bmatrix} \right| = -a_3 \neq 0.$$

Since D is an elementary divisor domain, there exist unimodular matrices U and V with coefficients in D such that

$$UMV = \begin{bmatrix} p_0' & 0 \\ 0 & p_3' \end{bmatrix}$$

with $p_0' | p_3'$. Using Lemma II. 6 with $W = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and

part (5) of Theorem II.7, it follows that D is a $\mathcal{B}$-domain.

Proposition 2: A Bezout domain is a $\mathcal{B}$-domain if and only if for any two forms $f,g \in \mathcal{P}(d)$ there exist $f_1 \in \bar{f}$ and $f_2 \in \bar{g}$ such that f_1 and f_2 have the same middle coefficients.

Proof: (=>) Clear

(<=) Suppose $f_1 = [a,B,c]$ and $f_2 = [a',B,c']$. From Chapter I, we can use Gauss's algorithm (Theorem I.8). Set $Q_1 = 1$ and $Q_0 = Q_2 = Q_3 = 0$ and we get

$$T = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ a/\lambda & 0 & 0 & -c'/\lambda \end{bmatrix}$$

as a transformation from f_3 into f_1f_2 where f_3 is a direct compound of f_1f_2 under T and $\lambda = (a,c')$. If $f_3 = [a_3,b_3,c_3]$, then $f_3 \sim [c_3,-b_3,a_3] = f_3'$ and f'_3 is a direct compound of f_1f_2 under

$$T' = \begin{bmatrix} a/\lambda & 0 & 0 & -c'/\lambda \\ -p_0 & -p_1 & -p_2 & -p_3 \end{bmatrix} .$$

Since $(a/\lambda, c'/\lambda) = D$, there exist $r,s \in D$ such that $(a/\lambda)r + [-(c'/\lambda)]s = 1$.

Since

$$\begin{bmatrix} 1 & 1 \\ (c'/\lambda)s & 1+(c'/\lambda)s \end{bmatrix} \begin{bmatrix} a/\lambda & 0 \\ 0 & -c'/\lambda \end{bmatrix} \begin{bmatrix} r & c'/\lambda \\ s & a/\lambda \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -ac'/\lambda^2 \end{bmatrix}$$

and $ac' \neq 0$, the proposition holds by part 5) of Theorem II.7 with $\alpha = 1$, $\beta = 0$.

Corollary 3: A Bezout domain is a $\mathcal{B}$-domain if and only if for any two forms $f_1, f_2 \in \mathcal{P}(d)$ there exists $f_i' = [a_i, b_i, c_i] \sim f_i$ for $i = 1,2$ such that $b_1 = -b_2$.

Proof: Use Proposition 2 and the fact that

$$[a_2, b_2, c_2] \sim [c_2, -b_2, a_2].$$

Corollary 4: If D is a Bezout domain, then united form composition holds for any primitive class with itself.

Proposition 5: A Bezout domain is a $\mathcal{B}$-Domain if and only if for two forms $f, g \in \mathcal{P}(d)$ one represents primitively an element of D that divides an element of D that is represented primitively by the other.

Proof: (=>) Clear.

(<=) We can assume $f = [at, b, c]$ and $g = [a, b', c']$. If $(a, (b + b')/2) = (m)$, then by Theorem I.8, setting $Q_0 = -1$, $Q_1 = Q_2 = Q_3 = 0$, we get a direct compound of f and g under the transformation

$$T = \begin{bmatrix} m & p_1 & p_2 & p_3 \\ 0 & ta/m & a/m & (b+b')/2m) \end{bmatrix}$$

$$= \begin{bmatrix} m & p_1 & p_2 & p_3 \\ 0 & tq_1 & q_1 & q_3 \end{bmatrix} .$$

As in Proposition 2, there exist r, $s \in D$ such that

$$(q_1 q_3)\begin{pmatrix} r & -q_3 \\ s & q_1 \end{pmatrix} = (1 \quad 0).$$

Therefore,

$$\begin{pmatrix} 0 & 1 \\ -1 & q_1 st \end{pmatrix}\begin{pmatrix} 0 & tq_1 \\ q_1 & q_3 \end{pmatrix}\begin{pmatrix} r & -q_3 \\ s & q_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -q_1^2 t \end{pmatrix}.$$

Hence the proposition follows by Theorem II.3

Proposition 6: If $f_i = [a_i, b_i, c_i]$ $(i = 1,2)$ are elements of $\mathcal{O}(d)$ with coefficients in any domain D such that $(a_1, a_2) = D$, then there exist $f_i' \in \bar{f}_i$ $(i = 1,2)$ such that f_1' and f_2' are united.

Proof: See [B-E, p. 162] for a proof.

The following are examples of Bezout domains that are elementary divisor domains (denoted EDDs). We have been unable to find a Bezout domain that is not an EDD. Examples of rings that are not domains, that are not elementary divisor rings, and that are rings with the property that finitely generated ideals are principal have been given in [GH2, 378]. These examples modulo a prime ideal, however, are EDDs.

If D is a Bezout domain with quotient field K and J is a domain such that $D \subset J \subset K$, then it is easy to show that J is also a Bezout domain. Furthermore, if P is a

prime ideal in a Bezout domain, then D/P is a Bezout domain. If $\{D_\alpha\}_{\alpha\in A}$ is a collection of Bezout domains such that if $\alpha_1,\alpha_2 \in A$, then there exists $\alpha_3 \in A$ such that $D_{\alpha_i} \subset D_{\alpha_3}$ for $i = 1,2$, then $D = \bigcup_{\alpha\in A} D_\alpha$ is a Bezout domain. However, the polynomial ring $D[x]$ is a Prüfer domain if and only if D is a field, as the following easy argument shows (D is a Prüfer domain provided every finitely generated ideal is invertible; hence a Bezout domain is Prüfer [GI, 253-386]). Suppose $D[x]$ is a Prüfer domain and let $0 \neq d \in D$. Then (d,x) is invertible and $(d,x) > (x)$ implies that $(d,x)Q = (x)$ for some ideal Q of $D[x]$. Since (x) is prime, then $Q = (x)$, $(d,x) = D[x]$, and d is a unit in D.

If D is an EDD with quotient field K and J is a domain such that $D \subset J \subset K$, then J is an EDD; we see this as follows. Let $a/b \in J$ with $a,b \in D$. Then $(a,b) = (d)$, $a = a_1d$, $b = b_1d$, $a_1x + b_1y = 1$ (all elements in D). Hence $(a_1x/b_1) + y = 1/b_1 \in J$; thus, if $\alpha \in J$, then $\alpha = a_1/b_1$ with $a_1,b_1 \in D$ and b_1 a unit in J. It now follows readily that 2x2 matrices over D can be diagonalized. Furthermore, it is clear that if P is a prime ideal in an EDD J, then J/P is an EDD; and the union of a family of EDDs forming a net (as for Bezout domains above) is an EDD.

We now give several examples of nontrivial EDDs.

Example 1: The ring D of algebraic integers is an EDD. If $(a,b,c) = D$, then there exist $a_1,b_1,c_1 \in D$ such that $aa_1 + bb_1 + cc_1 = 1$. Hence there exists a domain $D' \subset D$ such that $a,a_1,b,b_1,c,c_1 \in D'$ and D' is the integral closure of the integers in a finite algebraic extension field of the rationals. Furthermore, D' is a Dedekind domain (see [ZS1, Chapter 5] or [M] for details).

Therefore, by the proof of Proposition 2.1 in [BE, 156], there exists $k \in D'$ such that $(a,b+kc) = D'$. Since $(a,b + kc) = D$ when the ideal is extended to D and since D is Bezout (see [M, 85-86]) it follows that D is an EDD.

Example 2: The ring of entire functions D is an EDD. If $f(z) \in D$, then $f(z) = c\, z^m e^{\psi(z)} \prod f_k(z)$ by the Weierstrass representation of $f(z)$ where $f_k(z)$ is a monic, linear polynomial, the product is countable, the representation is within a unit factor and c is chosen so $\psi(0) = 0$ [H2, 346] and [SZ, 295-300]. It follows that each $f_k(z)$ is an irreducible element of D and that D is therefore an EDD (see [KA1, 473] for further details or [H1]).

Definition: We shall say that n is in the stable range of R if R is a ring such that for $(a_1,\ldots,a_s,a_{s+1}) = R$ with $s \geq n$, there exist $b_1,\ldots,b_s \in R$ such that $(a_1 + b_1a_{s+1}, a_2 + b_2a_{s+1},\ldots,a_s + b_sa_{s+1}) = R$ (see

[EO, 344-345]).

Example 3: If D is a Bezout domain and has 1 in its stable range, then D is an EDD. In [EO, 349], it is shown that if $a,b \in D$, then $(a,b) = (a+kb)$ for some $k \in D$. In addition if D is Bezout with 1 in its stable range and quotient field K and J is a domain such that $D \subset J \subset K$, then J has the same property [EO, 350].

Definition: A Kronecker function ring is defined as follows (see [EO, 347] or [GI, 356-377]): Suppose D is an integrally closed domain with quotient field K and suppose $\{R_r\}$ is the set of all valuation rings of K containing D and suppose v' is the trivial extension of v to $K(x)$ where x is an indeterminant over K, i.e., $v'(a_n x^n+\ldots+a_o) = \inf\{v(a_n),\ldots,v(a_o)\}$. If $R_{v'}$ is the valuation ring of v' and if $D' = \cap R_{v'}$, then D' is called the Kronecker function ring of D. We will often not reference D and will say D' is a Kronecker function ring.

Example 4: Kronecker function rings are EDD ([EO,347] or [GI, 367]).

Definition: A domain D has property F if each nonzero element of D is contained in at most a finite number of maximal ideals.

If D is an F-domain, then $(a,b,c) = D$ implies

$(a, b+kc) = D$ for some $k \in D$ [BE, 156]. Hence a Bezout domain which is an F-domain must be an EDD; in particular a PID is an EDD.

Example 5: A valuation ring is a domain in which the ideals are totally ordered under inclusion (see [ZS2], [GI], [B3], and [N] for examples and properties of valuation rings). It is easy to see that a valuation ring is an EDD. In addition, if $V_1, \ldots, V_n$ are valuation rings with quotient field K, then it can be shown that $D = \bigcap_{i=1}^{n} V_i$ is an F-domain and a Bezout domain (see [GI, 262] and [N, 38]) and consequently D is an EDD.

Example 6: The domains formed by Jaffard's "pullback theorem" ([J1], [J2], [GI]) are EDD. In fact, these domains have 1 in their stable range.

Suppose k is a field and G is a lattice ordered group. Let D' be the domain consisting of all formal sums $\{\sum_{i=o}^{n} a_i x^{\alpha_i} \mid a_i \in k, \alpha_i \in G\}$. Let K signify the quotient field of D'. Define $\varphi: D' \to G$ by $\varphi(\Sigma a_i x^{\alpha_i}) = \inf(\{\alpha_i\})_{i=1,\ldots,n}$. Extend φ to K by $\varphi(a/b) = \varphi(a) - \varphi(b)$ for $a/b \in K$. Then $D = \{X \in K \mid \varphi(X) \in G_+\}$ is a domain [GI].

Suppose $X, Y \in D$, $X \neq 0$, $Y \neq 0$. We can assume $X = \Sigma a_i x^{\alpha_i}$, $Y = \Sigma b_i x^{\beta_i}$ since X and Y differ from these by a unit. Suppose $\varphi(X) = \lambda$ and $\varphi(Y) = \mu$. Since $\varphi(x^{\lambda}/X) = \varphi(X/x^{\lambda}) = 0$, we have x^{λ}/X and X/x^{λ} are units of

D. Since $(x^\lambda/X)\cdot X = x^\lambda$ and $(X/x^\lambda)\cdot x^\lambda = X$, it follows that $(x^\lambda) = (X)$. Likewise, $(x^\mu) = (Y)$.

If $\lambda = \mu$, then $(x^\lambda, x^\mu) = (x^\lambda) = (x^\mu)$. If $\lambda \neq \mu$, then $(x^\lambda, x^\mu) = (x^\lambda + x^\mu)$ since $x^\lambda/(x^\lambda + x^\mu)$ and $x^\mu/(x^\lambda + x^\mu) \in D$. If $(x^\lambda, x^\mu) = (x^\lambda + x^\mu)$, then $u_1X = x^\lambda$, $u_2Y = x^\mu$ for u_1, u_2 units of D which implies $(X,Y) = (u_1X, u_2Y) = (u_1X + u_2Y) = (X + (u_2/u_1)Y)$ $= ((u_1/u_2)X + Y)$. If $(x^\lambda, x^\mu) = (x^\mu) = (x^\lambda)$, then $(X,Y) = (u_1X, u_2Y) = (u_2Y) = (u_1X)$. Either way 1 is in the stable range.

Example 7: If B is a Bezout domain and if K is the quotient field of B and x is an indeterminant over K and M is the maximal ideal of K[[x]], then $B + M = D$ is a Bezout domain. Furthermore, if B has the property that $(a,b,c) = B$ implies $(ap, bp + cq) = B$, then D has the same property.

If B is Bezout and if $M < A \subset D$ for A an ideal of D, then $A = A' + M$ where A' is an ideal of B and furthermore any set of generators of A' in B is a set of generators of A in D [GI, 560-561]. If A is an ideal of D and $A \subset M$ and if $(\alpha_1, \alpha_2) = A$, then the following argument will show A is principal.

Suppose $\alpha_1 = a_k x^k + a_{k+1}x^{k+1} + \ldots$ and $\alpha_2 = b_\ell x^\ell + b_{\ell+1}x^{\ell+1} + \ldots$ with $a_k \neq 0$, $b_\ell \neq 0$, and $\ell \geq k \geq 1$.

Since $\alpha_1 = a_k x^k u_1$, $\alpha_2 = b_\ell x^\ell u_2$ with u_1, u_2 units in D, then $(\alpha_1, \alpha_2) = (a_k x^k, b_\ell x^\ell)$. If $k < \ell$, then $(\alpha_1, \alpha_2) = (\alpha_1)$. Suppose $k = \ell$. We can assume $a_k = a_k'/m$ and $b_\ell = b_k = b_k'/m$ with $a_k', b_k', m \in B$. Since B is Bezout, $(a_k', b_k') = (c)$. It follows easily that $(\alpha_1, \alpha_2) = (cx^k/m)$ and D is Bezout.

Suppose $(\alpha, \beta, \gamma) = D$ with $\alpha = a_o + a_1 x + \ldots$, $\beta = b_o + b_1 x + \ldots$, and $\gamma = c_o + c_1 x + \ldots$. It is known that $k = k_o + k_1 x + \ldots$ is a unit of D if and only if k_o is a unit of B. ([N, 50] can be used to show this). Hence $(a_o, b_o, c_o) = D$, so there exist $p_o, q_o \in B \subset D$ such that $(a_o p_o, b_o p_o + c_o q_o) = B$. It follows easily that $(\alpha p_o, \beta p_o + \gamma q_o) = D$. Hence D is an EDD if B is.

This example says that an EDD of any finite dimension can be generated, e.g., for an initial B take any PID (such as the integers).

A similar argument can be used to show that D has 1 in its stable range if B does. Furthermore, if $\{D_\alpha\}_{\alpha \in A}$ is a net of Bezout domains with 1 in the stable range, then $D' = \bigcup_{\alpha \in A} D_\alpha$ is a Bezout domain with 1 in the stable range as the following argument shows. In [EO, 349], it is shown that a domain D is Bezout and has 1 in its stable range if and only if for any $a_1, a_2 \in D$ and $b \in (a_1, a_2)$, there exist $c, d \in D$ such that $b = c(a_1 + da_2)$.

Suppose $a_1, a_2 \in D'$ and $b \in (a_1, a_2)$. Then $b = a_1 m + a_2 n$. There exists $\beta \in A$ such that $b, a_1, a_2, m, n \in D_\beta$ and hence $b \in (a_1, a_2)$ in D_β. Therefore, there exist $c, d \in D_\beta \subset D'$ such that $b = c(a_1 + da_2)$ in D_β and hence in D'.

Example 8: Let K be an algebraically closed field of characteristic not 2. Let $x_1 = X$ be an indeterminant over K and suppose x_{n-1} is defined, then x_n is defined by $x_{n-1} = x_n^2$. The set of $K[x_n, \frac{1}{x_n}]$ forms a net and $\bigcup_{n=1}^{\infty} K[x_n, \frac{1}{x_n}]$ is an EDD. This example is given in [B4,86]. It is easily seen that $K[x_n]$ is a Euclidean domain and hence an EDD for n any natural number. If $\sum_{i=0}^{k} a_i (\frac{1}{x_n})^i$ and $\sum_{i=0}^{\ell} b_i (\frac{1}{x_n})^i$ are two nonzero elements of $K[x_n][\frac{1}{x_n}] = K[x_n, \frac{1}{x_n}]$ and $k \geq \ell$, then

$$(\tfrac{1}{x_n})^k [(x_n)^k (\Sigma a_i (\tfrac{1}{x_n})^i, \Sigma b_i (\tfrac{1}{x_n})^i)] = (\tfrac{i}{x_n})^k (\Sigma \lambda_i x_n^i, \Sigma \mu_i x_n^i)$$

$$= (\tfrac{1}{x_n})^k (\beta) = (\tfrac{\beta}{x_n^k}) \quad \text{where } \lambda_i, \mu_i \in K \text{ and } \beta \in K[x_i].$$

Hence $K[x_n, \frac{1}{x_n}]$ is a PID and thus an EDD. It follows therefore that $UK[x_n, \frac{1}{x_n}]$ is an EDD.

CHAPTER IV

COMPOSITION IN DOMAINS THAT MAY NOT BE BEZOUT

In this chapter we study composition in domains that may not be Bezout, and in particular investigate conditions under which information concerning composition locally (i.e., in the quotient rings D_P, for P a prime ideal of D) yields global information (i.e., in D itself). One of our main results is that $D[x]$ is a G-domain when D is a PID. We wish to thank Professor Dennis R. Estes for suggestions in this connection.

The relationship between binary quadratic forms over D and certain D-modules in a quadratic extension of the quotient field K of D has been developed as a useful technique in investigating properties of forms and D-modules (e.g., see [KA2] and [BE, 173-180] for recent applications and for other references). If $d = t^2 - 4n$ is a nonsquare discriminant in D, then $f(x) = x^2 - tx + n$ is an irreducible polynomial in the polynomial ring $D[x]$. The roots of $f(x)$ are $(t + \sqrt{d})/2$ and $(t - \sqrt{d})/2$ where $\sqrt{d}$ is a fixed root of the polynomial $x^2 - d$. If $\alpha,\beta \in K(\sqrt{d})$, then $D[\alpha,\beta]$ (or $[\alpha,\beta]D$) will be used to denote the D-module generated by α and β. If $\alpha = a + b\sqrt{d} \in K(\sqrt{d})$, then

$\bar{\alpha} = a - b\sqrt{d}$ is the conjugate of α, $N(\alpha) = \alpha\bar{\alpha}$ is the norm of α, and $T(\alpha) = \alpha + \bar{\alpha}$ is the trace of α. If $M \subset K(\sqrt{d})$ is a D-module, then $\bar{M}$ will denote the set of conjugates of M, and it is clear that $\bar{M}$ is also a D-module. We set $N(M) = M\bar{M}$, the product of M and $\bar{M}$ as D-modules in $K(\sqrt{d})$. If $f = [a,b,c]$ is a form over D of discriminant d, then we associate with f the D-module $M_f = D[a,(b+\sqrt{d})/2]$. It might be noted that it is important to always use $(b+\sqrt{d})/2$ (or to always use $(b-\sqrt{d})/2$) in our following arguments. It might also be noted that $K(\sqrt{d}) = K((b+\sqrt{d})/2) = K((b-\sqrt{d})/2)$, but $D[a,(b+\sqrt{d})/2]$ is equal $D[a,(b-\sqrt{d})/2]$ if and only if $a|b$.

Lemma 1: If T is a 2×4 matrix over D, then there exists a 4×2 matrix S over D such that $TS = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ if and only if T is primitive.

Proof: Let $T = (a_{ij})(i = 1,2;\ j = 1,2,3,4)$. If the ideal generated by the $D_{ij} = a_{1i}a_{2j} - a_{2i}a_{1j}$ $(1 \le i < j \le 4)$ is D, then there exist $u_i \in D$ $(i = 1,2,3,4)$ such that $\sum_{i=1}^{4} u_i a_{1i} = 1$ and $b_{ij} \in D$ $(1 \le i < j \le 4)$ such that $\sum b_{ij} D_{ij} = \sum_{i=1}^{4} u_i a_{2i}$. Set $x_{11} = u_1 + b_{12}a_{12} + b_{13}a_{13} + b_{14}a_{14}$, $x_{21} = u_2 - b_{12}a_{11} + b_{23}a_{13} + b_{24}a_{14}$, $x_{31} = u_3 - b_{13}a_{11} - b_{23}a_{12} + b_{34}a_{14}$, $x_{41} = u_4 - b_{14}a_{11} - b_{24}a_{12} - b_{34}a_{13}$. Then $\sum_{i=1}^{4} x_{i1}a_{1i} = 1$ and $\sum_{i=1}^{4} x_{i1}a_{2i} = 0$. Similarly, there exist

$x_{i2} \in D$ $(i = 1,\ldots,4)$ such that $\sum_{i=1}^{4} x_{i2}a_{2i} = 1$ and $\sum_{i=1}^{4} x_{i2}a_{1i} = 0$. It follows that $(a_{ij})\,(x_{ij}) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Conversely, suppose there is a matrix S over D such that $TS = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Let $W = \begin{bmatrix} a_{21} & a_{22} & a_{23} & a_{24} \\ -a_{11} & -a_{12} & -a_{13} & -a_{14} \end{bmatrix}$, where $T = (a_{ij})$. If W' denotes the transpose of W, then $W'T = (y_{ij})$ where $y_{ii} = 0$, $y_{ij} = -D_{ij}$ for $j > i$, and $y_{ij} = D_{ji}$ for $j < i$. Since $(W'T)S = W'$, it follows that the 2x2 subdeterminants of T generate D and T is primitive.

Q.E.D.

The next theorem extends Theorem 5.3 of [BE, 175]; while the proof is in part the same (the above lemma is part of the proof in [BE]), there is a point of difficulty to overcome and we include the entire proof for completeness.

Theorem 2: Let $f = [a,b,c]$ and $g = [a',b',c']$ be primitive binary quadratic forms over a domain D (characteristic not 2) with nonsquare discriminant d. The following are equivalent.

1) There exists a direct compound of fg over D.
2) The D-module M_fM_g is generated by two elements and $b \equiv b' \bmod(2)$.
3) M_fM_g is a free D-module and $b \equiv b' \bmod(2)$.

4) $M_f M_g$ is a free two dimensional D-module and $b \equiv b' \bmod(2)$.

Proof: 1)=> 2) Suppose there exists a direct compound h of fg under a primitive bilinear transformation

$$T = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix} .$$

Set

$$\alpha_1 = a'q_1 - q_0(b' + \sqrt{d})/2, \quad d_2 = -a'p_1 + p_0(b' + \sqrt{d})/2 .$$

The elements in the matrix $[\alpha_1 \alpha_2]$ T are the generators of the D-module $M_f M_g$, and consequently $M_f M_g \subset [\alpha_1, \alpha_2]D$. Since T is a primitive matrix, there exists a 4x2 matrix

$$V = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ y_0 & y_1 & y_2 & y_3 \end{bmatrix}'$$

over D such that $TV = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Hence $[\alpha_1 \alpha_2]TV = [\alpha_1 \alpha_2]$ and $M_f M_g = [\alpha_1, \alpha_2]D$. Furthermore, $b \equiv b' \bmod(2)$ by Lemma I.18.

2)=> 3) Since d is nonsquare, it follows that the two elements aa' and $a(b' + \sqrt{d})/2$ are nonzero and linearly independent over K, and consequently linearly independent over D. It follows therefore that $M_f M_g$ is free since it is generated by two elements.

3)=> 4) Since $M_f \cdot M_g$ can be generated by four elements, it follows that it has a finite basis. Since a

set of linearly independent elements of M_fM_g is a set of linearly independent elements of the two dimensional vector space $K(\sqrt{d})$ over K, it follows that M_fM_g must have a basis of two elements (recall that M_fM_g contains two linearly independent elements).

4)=> 1) Suppose $\alpha_1\alpha_2$ are such that $M_fM_g = D[\alpha_1\alpha_2]$ where α_1 and α_2 are linearly independent. Let $U = [aa', a(b'+\sqrt{d})/2, a'(b+\sqrt{d})/2, ((b+\sqrt{d})/2)((b'+\sqrt{d})/2)]$ be the 1x4 matrix whose entries are the "natural" generators of M_fM_g obtained by multiplying M_f and M_g as D-modules. There exists a matrix

$$T = \begin{bmatrix} p_0 & p_1 & p_2 & p_3 \\ q_0 & q_1 & q_2 & q_3 \end{bmatrix} ,$$

with entries in D such that $U = [\alpha_1\alpha_2]\,T$. Let W denote the transpose of $[X_1X_2 \;\; X_1Y_2 \;\; Y_1X_2 \;\; Y_1Y_2]$ and $[X \;\; Y]$ the transpose of TW. Then $[\alpha_1 \;\; \alpha_2]\,[X\;Y]' = UW$ and therefore $(aX_1 + (b+\sqrt{d})/2\,Y_1)(a'X_2 + (b'+\sqrt{d})/2\,Y_2) = \alpha_1X + \alpha_2Y$. Taking norms we have $af\cdot a'g = \alpha_1\bar{\alpha}_1X^2 + (\alpha_1\bar{\alpha}_2 + \bar{\alpha}_1\alpha_2)XY + \alpha_2\bar{\alpha}_2Y^2$, and the form $h = [\alpha_1\bar{\alpha}_1/aa', (\alpha_1\bar{\alpha}_2 + \bar{\alpha}_1\alpha_2)/aa', \alpha_2\bar{\alpha}_2/aa']$ is transformed into fg under T. It is clear that h has coefficients in K, the quotient field of D; and we claim that h has coefficients in D. It is clear that $aa'h$ has coefficients in $[\alpha_1,\alpha_2][\bar{\alpha}_1,\bar{\alpha}_2]\,D = M_f\bar{M}_fM_g\bar{M}_g$. Using the fact that $(a,b,c) = D$ and $(a',b',c') = D$, we have

$M_f\bar{M}_f = a[1,(b+\sqrt{d})/2]D$ and $M_g\bar{M}_g = a'[1,(b'+\sqrt{d})/2]D$.
Hence h has coefficients in the D-module
$MM' = [1,(b+\sqrt{d})/2][1,(b'+\sqrt{d})/2]D$. Since $1,\sqrt{d}$ are linearly independent over K, if $r \in MM' \cap K$, then there exist $u,v,x,y \in D$ such that

(1) $r = x + y(b/2) + u(b'/2) + v(bb'+d)/4$ and

(2) $0 = y + u + v(b+b')/4$.

Solving for y in (2) and substituting into (1) we obtain

(3) $r = x + u(b'-b)/2 + vac.$

Since $b \equiv b' \bmod(2)$ in D, it follows that $r \in D$ and consequently the form h has coefficients in D as asserted. Let V be the matrix over D such that $[\alpha_1\ \alpha_2] = UV$. Since α_1 and α_2 are linearly independent over D and $U = [\alpha_1\alpha_2]T$, it follows that $TV = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and T is primitive. Therefore, h is a compound of fg and there exist units r_1, r_2 of D such that $r_1 = \pm r_2$ and the conditions of Proposition I.1 are satisfied. Since d is nonsquare in D, $a \neq 0$ and one of p_o, q_o is not zero - say $q_o \neq 0$. Now $aa' = \alpha_1 p_o + \alpha_2 q_o$ and $a(b'+\sqrt{d})/2 = \alpha_1 p_1 + \alpha_2 q_1$ and solving for α_1 gives $r_1\alpha_1 = a'q_1 - q_o(b'+\sqrt{d})/2$. Similarly, $r_2\alpha_1 = a\,q_2 - q_o(b+\sqrt{d})/2$ and it follows that $r_1 = r_2$, since $r_1 = -r_2$ implies $q_o\sqrt{d} = 0$. Replacing α_2 by $r_1\alpha_2$ and $b = [a_1, b_1, c_1]$ by $h_1 = [a_1, r_1 b_1, r_1^2 c_1]$, and

q_i with q_i/r_i $(i = 0,1,2,3)$, it follows that h_1 is a direct compound of fg.

Theorem 3: If D is an F-domain and $f,g \in \mathcal{P}(d)$ are such that their middle coefficients are congruent mod (2) in D, then there exist united forms f',g' with $f' \sim f$ and $g' \sim g$.

Proof: Same as that of Theorem 3.3 in [BE, 162].

Theorem 4: Let D be a domain such that finitely generated projective D-modules are free, and let $f,g \in \mathcal{P}(d)$ be such that their middle coefficients are congruent mod (2) in D. Then there exists a direct compound of fg over D.

Proof: Suppose $f = [a,b,c]$ and $g = [a',b',c']$ are two primitive forms over D with nonsquare discriminant d. Since $(a,b,c) = D$, it follows that $(a,b,c)D_M = D_M$ when considered as an ideal in the quotient ring D_M, where M is a maximal ideal of D [251, 219], and hence $[a,b,c]$ is a primitive form over D_M. Likewise, $[a',b',c']$ is a primitive form over D_M. Now f is associated with the D-module $D[a,(b + \sqrt{d})/2]$ and g with the D-module $D[a',(b' + \sqrt{d})/2]$.

It follows that $D_M[a,(b + \sqrt{d})/2]$ is the D_M-module associated with the form $[a,b,c]$ over D_M and also that $D_M[a,(b + \sqrt{d})/2]$ is $D_M \cdot D[a,(b + \sqrt{d})/2]$. Furthermore

$D_M(D[a,(b+\sqrt{d})/2]\cdot D[a',(b'+\sqrt{d})/2]) =$

$D_M[a,(b+\sqrt{d})/2]\cdot D_M[a',(b'+\sqrt{d})/2]$. Since D_M is an F-domain and $b \equiv b' \bmod (2)$, it follows by Theorem 3 that there exists a direct compound of $[a,b,c]$ and $[a',b',c']$ over D_M. Hence by Theorem 2, $D_M[a,(b+\sqrt{d})/2]\cdot D_M[a',(b'+\sqrt{d}/2]$ is a free two dimensional module and hence $D_M(M_f M_g)$ is a two dimensional free module for all maximal ideals of D. Therefore, $M_f M_g$ is a finitely generated projective D-module [Bl, 141]. Therefore $M_f \cdot M_g$ is a free D-module by hypothesis and, by Theorem 2, there exists a direct compound of $f\cdot g$.

Corollary 5: If D is a domain such that finitely generated projective D-modules are free, and such that for each maximal ideal M of D the quotient ring D_M is a G-domain, then D is a G-domain.

Proof: Clear from the proof of Theorem 4 and the fact that $(b - b')/2 \in D$ if $(b - b')/2 \in D_M$ for each maximal ideal M of D [N, 23].

Corollary 6: If D is a PID, then D[x] has property G. (In particular Z[x] is a G-domain).

Proof: By Seshadri's theorem [SES, 456-457], if M is a finitely generated projective D[x]-module for D a PID, then M is free.

Since D is a PID, it follows that D is integrally closed and hence $D[x]$ and $D[x]_P$ are integrally closed for P a prime ideal of $D[x]$ [ZS1, 261]. Therefore, $D[x]_M$ is an F-domain with property C and hence a $\mathcal{B}$-domain by Theorem 3. Therefore, $D[x]_M$ is a G-domain for every maximal ideal M in D and $D[x]$ is a G-domain by Corollary 65.

Remark: Although $D[x]$ is a G-domain for D a PID, we have been unable to show whether or not $D[x]$ is a $\mathcal{B}$-domain (even in the case $D = Z$).

Definition: Let D be a local domain of dimension 1 with maximal ideal m. Let $\bar{D}$ be the integral closure of D in K, the quotient field of D, and let $\bar{n}$ be the Jacobson radical of $\bar{D}$. Then D is said to be a weak (discrete) valuation ring if we have $m = \bar{n}$ in the set-theoretical sense.

Definition: A Noetherian domain D is said to be a weakly normal ring provided

1) For any prime ideal P of height 1 in D, D_P is a weak valuation ring.
2) Any principal ideal ($\neq 0$) has the property that its prime divisors have height 1 in D.

The above definitions are from [EN, 341] and [N] gives terms not defined above.

Proposition 7: If D is a semi-local, weakly normal ring of dimension 1, then $D[x,y]$, where x and y are indeterminants over D, has the property that finitely generated projective modules are free. (In particular, if $D_{v_1},\ldots,D_{v_n}$ are rank 1, discrete valuation rings with a common quotient field, then $D = \bigcap_{i=1}^{n} D_{v_i}$ satisfies the above hypothesis).

Proof: See [EN, 351-352].

Corollary 8: If D is a semi-local, weakly normal ring of dimension 1, then $D[x,y]$, where x and y are indeterminants over D, has the property that a direct compound exists for any two primitive forms whose middle coefficients are congruent mod (2).

Proof: Easy, using Proposition 7, Theorem 4, and the proof of Corollary 6.

Corollary 9: If D is the intersection of a finite number of rank 1, discrete valuation rings having a common quotient field, then $D[x,y]$ is a G-domain where x and y are indeterminants. (In particular, if $p_1,\ldots,p_n$ are primes in Z and if $S = Z\setminus(p_1,\ldots,p_n)$, then $Z_S[x,y]$ is a G-domain).

Proof: Immediate from Corollary 8. It should be noted that D is a PID and that $Z_S = \bigcap_{i=1}^{n} Z_{(p_i)}$ (see [N, 37-38]).

Theorem 10: If D is a domain, then a necessary and sufficient condition for D to be an F-domain is that D_S be an F-domain where S is a multiplicative system of D containing a unit.

Proof: It follows easily from the elementary properties of quotient rings that D_S is an F-domain when D is. ([ZS1, 218-233] provides a treatment of quotient rings).

Suppose that D_S is an F-domain for each quotient ring D_S such that $D_S > D$. For each nonzero x in D denote by F_x the family of maximal ideals in D containing x and by F'_x the family of maximal ideals of D which do not contain x, and denote the Jacobson radical of D by $J(D)$.

If every nonunit of D is in $J(D)$, then $J(D)$ is the unique maximal ideal of D and D is an F-domain.

Let x be a nonunit of D such that $x \notin J(D)$. Then there is a maximal ideal M such that $x \notin M$, and hence there is $m \in M$ such that $(x,m) = D$. If $S = \{m^n | n = 0,1,2,\ldots\}$, then $D_S > D$ and $M'D_S \neq D_S$ for $M' \in F_x$. Hence F_x is finite. Consequently, if $J(D) = (0)$, then D is an F-domain. Suppose $y \in J(D)$ with $y \neq 0$, and let $S' = \{x^n | n = 0,1,2,\ldots\}$. Now $D_{S'} > D$, $M''D_{S'} \neq D_{S'}$ for $M'' \in F'_x$, $y \in M''$ for $M'' \in F'_x$, so that F'_x is finite. Thus if $J(D) \neq (0)$, there are only a finite number of

maximal ideals in D, and D is an F-domain.

Remark: In the proof of the converse of Theorem 10, we only need to know that D_S is an F-domain for multiplicative systems S of the form $S = \{x^n | n = 0,1,\ldots\}$ where $x \neq 0$ is a nonunit of D.

The following are some examples of F-domains: PID's Dedekind domains, valuation rings, the intersection of a finite number of valuation rings with a common quotient field, $K[x,y]/(y^2 - f^2(x)g(x))$ where K is a field $(2 \neq 0)$ with f and g nonconstant polynomials in $K[x] \subset K[x,y]$ with g square free, any quasi-semi-local domain, any Noetherian domain that is one dimensional, any quotient overring of an F-domain (see above), Nagata's example of a Noetherian domain whose height is infinite [N, 203], and $D[[x]]$ where D is local or semi-local.

Definition: If A is an ideal of a ring R, then let $J(A)$ denote the intersection of the maximal ideals containing A and let $J = \{\text{ideals } A \text{ of } R | J(A) = A\}$. A ring R is J-Noetherian provided the ideals of J satisfy the ascending chain condition (denoted a cc). A prime ideal P in J which contains an ideal A of R is called a J-component of A if P is minimal among the primes of J containing A.

If R is J-Noetherian, then every ideal of R has only finitely many J-components. (See [EO, 344] for details

and references).

Proposition 11: If D is a one-dimensional domain, then a necessary and sufficient condition for D to be J-Noetherian is that every nonzero ideal of D be contained in at most a finite number of maximal ideals.

Proof: Suppose D is J-Noetherian. Then a nonzero ideal A is contained in only finitely many J-components and since D is one-dimensional, the J-components of A are the maximal ideals containing A.

Suppose each nonzero ideal of D is contained in only a finite number of maximal ideals. Then $A \in J$ if and only if $A = (0)$ or A is a finite intersection of maximal ideals. Hence D is J-Noetherian.

Corollary 12: If D is a 1-dim. domain, then D is J-Noetherian if and only if D is an F-domain.

Proof: (=>) Clear from Proposition 11.

(<=) If $A \in J$ and $A \neq (0)$, then there exists $0 \neq a \in A$ and a is contained in at most a finite number of maximal ideals and hence so is A.

Remark: The example in [BE, 177] is 2-dim. and J-Noetherian, but is not an F-domain.

Theorem 13: Let D[x] be a G-domain and consider the set

$C(d(x))$ of classes of primitive binary quadratic forms over $D[x]$ with nonsquare discriminant $d(x) \in D[x]$ and let $C(d(0))$ denote the collection of classes of forms over D with discriminant $d(0)$. Define $\varphi: C(d(x)) \to C(d(0))$ as follows: If $f(x) = [a(x),b(x),c(x)]$ is a form in a class $\overline{f(x)}$ in $C(d(x))$, then $\varphi(\overline{f(x)}) = \overline{[a(0),b(0),c(0)]}$. Then φ is a homomorphism from $C(d(x))$ into $C(d(0))$.

Proof: If $h(x)$ and $g(x)$ are two forms over $D[x]$ and are elements of $\mathcal{P}(d(x))$ and $h(x) \sim g(x)$, then there exists a unimodular transformation $T(x) = \begin{bmatrix} r(x) & u(x) \\ s(x) & v(x) \end{bmatrix}$ from $h(x)$ to $g(x)$. It follows that $T(0) = \begin{bmatrix} r(0) & u(0) \\ s(0) & v(0) \end{bmatrix}$ is a transformation from $h(0)$ to $g(0)$. Furthermore $|T(x)| = 1$ implies $|T(0)| = 1$. If $h(x)$, $f(x)$, $g(x)$ are three forms over $D[x]$ of discriminant $d(x)$ and if

$$T(x) = \begin{bmatrix} p_0(x) & p_1(x) & p_2(x) & p_3(x) \\ q_0(x) & q_1(x) & q_2(x) & q_3(x) \end{bmatrix}$$

is a bilinear transformation from $h(x)$ into $f(x)g(x)$

then $$T(0) = \begin{bmatrix} p_0(0) & p_1(0) & p_2(0) & p_2(0) \\ q_0(0) & q_1(0) & q_2(0) & q_3(0) \end{bmatrix}$$

is a bilinear transformation from $h(0)$ into $f(0)g(0)$.

Q.E.D.

In [D1,134-140] and [BE,160-167], one of the basic results used in creating united forms is that a form can represent primitively an element relatively prime to a given element. We state this result explicitly below and show the result is false for the domain Z[x].

Example 1: The domain Z[x] does not have the following property. If $f = [a,b,c]$ is a form over D, E an ideal of D, $(a,b,c) \neq (0)$, $E \neq (0)$, and $(a,b,c) + E = D$, then there exists $r,s \in D$ such that $(ar^2 + brs + cs^2) + E = D$. (See [BE, 157]).

Let $h = [7,2x,10(x^2+1)]$ be a form over D. The discriminant of h is $4(-69x^2 - 70)$. The form h is primitive since $-7\cdot 7 + (-25x)2x + 5(10\cdot(x^2+1)) = -49-50x^2 + 50x^2 + 50 = 1$. The polynomial $f(y) = y^2 - (2x)y + 70(x^2+1)$ in $(Z[x][y]$ is irreducible by Eisenstein's criterian since $2\nmid 1, 2 \mid 2x, 2 \mid 70(x^2+1)$, $4 \nmid 70(x^2+1)$ [V,250]. There do not exist $c,d \in Z[x]$ such that $(7c^2+2xcd + 10(x^2+1)d^2) + (x) = Z[x]$ by the following argument. Suppose there exist $c,d,e,f \in Z[x]$ such that $7[7c^2 + 2xcd + 10(x^2+1)d^2] + ex = 1$ where $c = c_o + c_1x + \ldots + c_{n_c}x^{n_c}$, $d = d_o + d_1x + \ldots + d_{n_d}x^{n_d}$, etc. Then $f_o(7e_o^2 + 10d_o^2) = 1$ and hence $f_o = 1$ and $7e_o^2 = 10d_o^2 = 1$ since $7e_o^2 + 10d_o^2 > 0$. We need only show that $7m^2 + 10n^2 \neq 1$ for $m,n \in Z$, but that is clear.

It should be noted that the above property holds whenever E is contained in at most a finite number of maximal ideals regardless of the domain (see proof in [BE, 157]).

Example 2: There exists a form in $Z[x]$ whose form of constant terms represents 1, but it does not. This shows there exists more equivalence classes of forms of a certain discriminant in $Z[x]$ than in Z.

Let $h = [x, 2(x^2-1), 3(x+1)]$. Then h is primitive since $(-2x-3)x + 1\cdot(2(x^2-1)) + 1\cdot(3\cdot(x+1)) = 1$. Also, we have $f(y) = y^2 - 2(x-1)(x+1)y + 3x(x+1)$ is irreducible in $(Z[x])[y]$ by Eisenstein's criterian [V,250]. The form of the constant terms is $[0,-2,3]$, is primitive, and represents 1 since $1 = 0\cdot 1^2 - 2\cdot 1\cdot 1 + 3\cdot 1^2$; however its discriminant is a square. On the otherhand h does not represent 1 by the following argument. Suppose there exist $c,d \in Z[x]$ such that $xc^2 + 2(x^2-1)cd + 3(x+1)d^2 = 1$. Now $-2c_od_o + 3d_o^2 = 1$ implies $(-2c_o + 3d_o)d_o = 1$ which implies $d_o = \pm 1$ and $c_o = -d_o$. On the otherhand, $c_o^2 - 2(2c_od_o) + 3(2d_od_1) + 3d_o^2 = 0$; $1 + 4 + 6(\pm d_1) + 3 = 0$; $\pm 6d_1 = 8$. If $d_1 \neq 0$, then $3 \nmid 8$ which is impossible. If $d_1 = 0$, then $8 = 0$ which is also impossible. Therefore, h does not represent 1.

BIBLIOGRAPHY

[B1] N. Bourbaki, Éléments de Mathematic, Algèbre Commutative, Chapters 1 and 2, Herman, Paris, 1961.

[B2] _____, Éléments de Mathématique, Algèbre Commutative, Chapters 3 and 4, Herman, Paris, 1961.

[B3] _____, Éléments de Mathématique, Algèbre Commutative, Chapters 5 and 6, Herman, Paris, 1964.

[B4] _____, Éléments de Mathématique, Algèbre Commutative, Chapter 7, Herman, Paris, 1965.

[BE] H. S. Butts and D. Estes, Modules and binary quadratic forms over integral domains, Linear Algebra and its Applications 1 (1968), 153-180.

[D1] L. E. Dickson, Introduction to the Theory of Numbers, Dover, New York, 1957.

[D2] _____, History of the Theory of Numbers, vol. 3, The Carnegie Institution, Washington, 1923.

[DD] Dirichlet-Dedekind, Zahlentheory, ed. 2, Vieweg, Braunschweig, 1871.

[EN] S. Endo, Projective modules over polynomial rings, J. Math. Soc. Japan 15(1963), 339-352.

[EO] D. Estes and J. Ohm, Stable range in commutative rings, J. Algebra 7(1967), 343-362.

[G] C. F. Gauss, Disquisitiones Arithmeticae, Yale University, New Haven, 1966.

[GH1] L. Gillman and M. Henriksen, Some results about elementary divisor rings, Trans. Amer. Math. Soc. 82(1956), 362-365.

[GH2] _____, Rings of continuous functions in which every finitely generated ideal is principal, Trans. Amer. Math. Soc. 82(1956), 366-391.

[GI] R. W. Gilmer, Multiplicative Ideal Theory, Queen's University, Kingston, Ontario, 1968.

[H1] O. Helmer, The elementary divisor theorem for certain rings without chain condition, Bull. Amer. Math. Soc. 49(1943), 225-236.

[H2] _____, Divisibility properties of integral functions, Duke Math. J. 6(1940), 345-356.

[J1] P. Jafford, Contributions à l'étude des grouppes ordonnés, J. Math. Pures Appl. 32(1953), 203-280.

[J2] _____, Les Systems d'ideaux, Dunod, Paris, 1960.

[KA1] I. Kaplansky, Elementary divisors and modules, Trans. Amer. Math. Soc. 66(1949), 464-491.

[KA2] _____, Composition of binary quadratic forms, Studia Math. 5(1968), 523-530.

[LA] S. Lang, Algebra, Addison-Wesley, Reading, 1967.

[M] H. B. Mann, Introduction to Algebraic Number Theory, Ohio State University, Columbus, 1955.

[N] M. Nagata, Local Rings, Interscience, New York, 1962.

[P] G. Pall, Composition of binary quadratic forms, Bull. Amer. Math. Soc. 54(1948), 1171-1175.

[SZ] S. Saks and A. Zygmund, Analytic Functions, Polish Scientific, Warszawa, 1965.

[SES] C. S. Seshadri, Triviality of vector bundles over the affine space K^2, National Academy of Science 44(1958), 456-458.

[S] H. J. S. Smith, Collected Mathematical Papers, vol. 1, Chelsea, Bronx, 1965.

[V] B. L. van der Waerden, Modern Algebra, Frederick Ungar, New York, 1953.

[ZS1] O. Zariski and P. Samuel, Commutative Algebra, vol. 1, van Nostrand, Princeton, 1965.

[ZS2] _____, Commutative Algebra, vol. 2, van Nostrand, Princeton, 1960.

BIOGRAPHY

Bill J. Dulin was born on April 8, 1935, in Wink, Texas. He attended public schools in Kermit, Texas. In 1956, he received the Bachelor of Arts degree in Philosophy from Baylor University. He worked for Texaco, Inc., in Houston, Texas, before entering Louisiana State University in September 1964. He received the Master of Science degree in Mathematics at Louisiana State University in August, 1966, and is currently a candidate for the degree of Doctor of Philosophy in the Department of Mathematics.

EXAMINATION AND THESIS REPORT

Candidate: Bill J. Dulin

Major Field: Mathematics

Title of Thesis: Composition of Binary Quadratic Forms over Integral Domains

Approved:

H. S. Butts

Major Professor and Chairman

R D Anderson

Dean of the Graduate School

EXAMINING COMMITTEE:

J R Rathmford

J E Kiesler

L J Wade

F. F. Connor

Date of Examination:

May 13, 1969